STATE OF NEBRASKA

STATE PURCHASING BUREAU

NG9-1-1 ESInet and NGCS
Attachment C; Option C
RFP #: 6264 Z1

June 3, 2020

HAMILTON NG911

1006 Twelfth Street • Aurora, Nebraska 68818
voice 402.694.5101 • TTY 800.821.1834
toll free 800.821.1831 • fax 402.694.2848
e-mail: info@hamiltontel.com
web site: www.hamiltontel.com

June 3, 2020

Annette Walton / Nancy Storant, Buyer(s)
State Purchasing Bureau
1525 K Street, Suite 130
Lincoln, NE 68508

RE: Hamilton NG911's response to Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) RFP (RFP 6264 Z1)

Hamilton NG911, Inc. (Hamilton), a division of Hamilton Telecommunications and a Nebraska Corporation, is pleased to provide this response to all elements of the Nebraska Next Generation 911 Emergency Services (ESInet) and Next Generation Core Services (NGCS) RFP. Our proposals include separate, and complete, responses for the following options: Option B – NGCS and Option C – ESInet and NGCS. Such answers to the completed Corporate Overview, Sections II through IV, and technical requirements (Attachment C – Option B and C) are reflected in blue text.

Hamilton has a long history of experience in the telecommunications industry, starting in 1901 as a local telephone company. Since then, Hamilton has grown to encompass eight primary company divisions and operates on a local, regional and national basis. Hamilton Telephone Company started offering 9-1-1 service in 1968, added Hamilton Long Distance Company as an interexchange carrier (IXC) carrier in 1995, and has been a provision coordinator of wide area network (WAN) services for the past 20 years. Additionally, Hamilton Relay, sister company to Hamilton NG911, is a nationally FCC certified Traditional Relay and Captioned Telephone Service (TRS) provider.

Hamilton has great breadth in its experience, people, and resources. This is certainly true in working with state entities and supplying services through contracts such as the request for NG 9-1-1 services by the state of Nebraska. Hamilton knows how to fulfill contractual requirements and we are proud of the relationships we have built and maintained over the years. More importantly, Hamilton has a proven track record of responding to the needs of our customers, state regulatory bodies and other industry-related organizations efficiently and effectively.

The following individual is authorized to answer questions or provide clarification to the proposal.

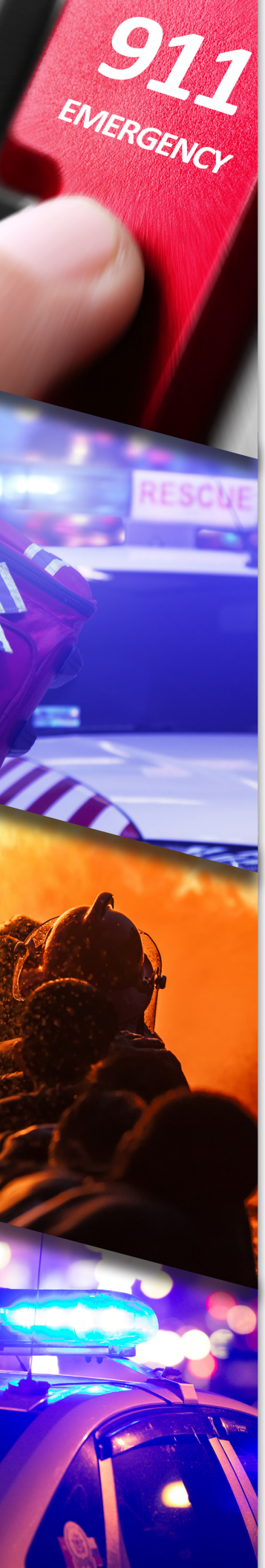
Ryan Wineteer
NG911 Manager
Hamilton NG911, Inc.
1006 12th Street
Aurora, Nebraska 68818
Voice: 402-694-7317
Email: ryan.wineteer@hamiltontel.com

Additionally, through subcontractor agreements, we are collaborating with **Communications Venture Corp. (d/b/a INdigital), Geo-Gomm, Inc., Digital Data Technologies Inc. (DDTI),** and **NebraskaLink Holdings, LLC** to successfully meet your requirements. Together, with these industry-leading companies in Public Safety, we have assembled a comprehensive solution that delivers the experience, dedication, reliability, and innovation to deliver a best-in-class NG 9-1-1 solution.

Hamilton acknowledges that it has received the following addendums: Addendum 1; Addendum 2; Addendum 3 – Revised Schedule of Events; Addendum 4, Questions and Answers; Addendum 5 – Revised Schedule of Events; Addendum 6 for Questions and Answers, Round Two; Addendum 7 for Questions and Answers, Additional Questions; and Addendum 8.

Hamilton has the relevant experience to ensure success for the state of Nebraska in this NG 9-1-1 project. We are committed to delivering the very best and our implementation will be seamlessly deployed by our experienced, trusted staff.

<<PROPRIETARY OR CONFIDENTIAL INFORMATION INTENTIONALLY REMOVED>>



REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

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

CONTRACTOR MUST COMPLETE THE FOLLOWING

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.

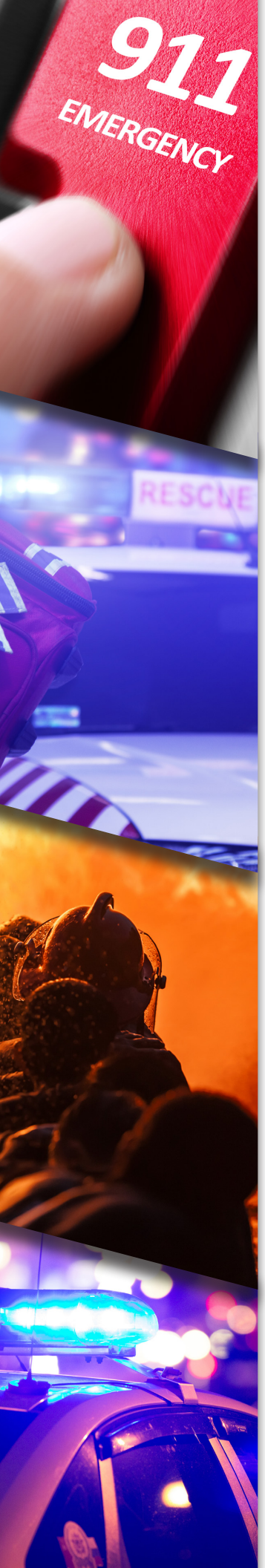
JN NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date 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:	**Hamilton NG911, Inc.**
COMPLETE ADDRESS:	**1006 12th Street, Aurora, NE 68818**
TELEPHONE NUMBER:	**402-694-5101**
FAX NUMBER:	**402-694-7317**
DATE:	**June 2, 2020**
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	**John Nelson, President**



EXECUTIVE SUMMARY

HAMILTON®
NG911

NEXT GENERATION 9-1-1

SERVICES AND SOLUTIONS

EXECUTIVE SUMMARY OF HAMILTON NG911

INTRODUCTION

Hamilton offers trusted and reliable NG 9-1-1 services, utilizing a robust infrastructure and experience in mission-critical IT service and support. Hamilton is dedicated to providing Public Safety Answering Points (PSAPs) and carriers with a top-level 9-1-1 service that allows emergency communications networks to accommodate modern communication methods.

WHY HAMILTON NG911?

Since 1901, Hamilton Telecommunications has been delivering telecommunications and technology services. As an established and trusted provider, Hamilton is committed to ensuring that we deliver the latest in technology with personalized customer service.

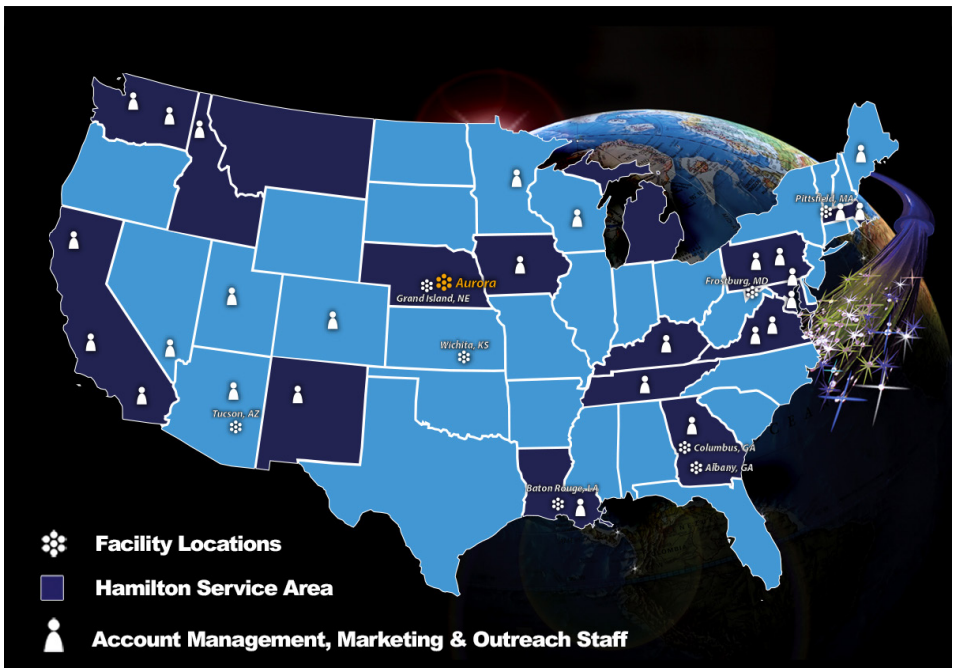
Hamilton NG911 provides:

- Real-Time Text (RTT) Technology
- SMS Text to 9-1-1
- Next Generation Core Services (NGCS)
- Extensive regulatory experience
- Broad understanding of accessibility components
- 24x7x365 cloud security through the Hamilton Tier 3 data center
- Contracted telecommunications service experience on local, state and regional levels

Hamilton brings experience in managing reliable networks, along with industry-leading experience that stretches beyond the scope of emergency services. Hamilton Relay®, a division of Hamilton Telecommunications, has been providing telecommunications relay services for individuals who are deaf, hard of hearing, deaf-blind or have difficulty speaking since 1991. Hamilton provides contracted Traditional Relay and Captioned Telephone service through 21 contracts to 15 states, the District of Columbia and the Island of Saipan, and is a provider of internet-based Captioned Telephone services nationwide.

Hamilton is a leading organization for delivering these critical services. Continued emphasis on innovation and expansion has made Hamilton a front-runner in the telecommunications industry.

Hamilton NG911
meets the needs of modern-day emergency communications with a focus on next-generation innovations.



Hamilton Service Area Map

SOLUTIONS & CERTIFICATIONS

NEXT GENERATION CORE SERVICES

An i3 Emergency Services IP Network (ESInet) providing PSAPs the capabilities to receive video, texts, photos, alarm signals and more. Through IP transport infrastructure, core functional processes can be deployed that are necessary for providing NG 9-1-1 services, ensuring PSAPs operate at the highest level.

TEXT SOLUTIONS

Allowing PSAPs to add non-voice (SMS), MMS and RTT to existing 9-1-1 services. Provides capability to receive text from all wireless carriers and end-users on one platform.

MEVO(+)

A premier, secure RTT solution for the Next Gen PSAP. MEVO(+) delivers a standards-compliant, RTT-capable VoIP solution that can be used to complement to the equipment and software on existing PSAP networks. This specialized system has been developed to deliver RTT technology, automatic location identification (ALI) as well as a secure failover, call-taking solution.

MEVO(+)

CYBERSECURITY

Providing 24x7x365 network security, preventative maintenance and monitoring under the National Institute of Standards and Technology (NIST) specifications. The solutions provided by Hamilton ensure workstations are equipped with a trusted infrastructure, and your operation is secure.

HAMILTON NETWORK SENTINEL

DATA ANALYTICS

A customizable data analytics solution provides call statistics and visualizations to effectively operate a PSAP. These tools provide accurate and timely information, flagging predefined events and anomalies requiring immediate action.

CUSTOMER PREMISE EQUIPMENT (CPE)

Robust hardware and software solutions that deliver multiple platform capabilities and are compliant with NENA i3 standards.

Features include:

- NG 9-1-1 Call Processing System
- Mapping and Data Tracking
- Logging and Reporting System
- 12, 24 and 48 Switch Models
- And More

Hamilton is a proven, trusted provider and is committed to delivering the latest in technology and personalized customer service.

A TEAM OF EXPERTS

Working closely with a team of industry experts ensures Hamilton provides the most complete NG 9-1-1 services available.

HAMILTON®

NOTABLE PERFORMANCES

A current three-year, million-dollar transport and bandwidth agreement with a major national internet provider.

Providing network design, support and maintenance for numerous companies with annual revenues ranging from $100,000 to $1,000,000,000.

For over 20 years, Hamilton has been providing core network services and network monitoring for numerous Nebraska telephone and internet service providers.

Supplying contracted Traditional Relay and Captioned Telephone service through 37 contracts over 27 years.

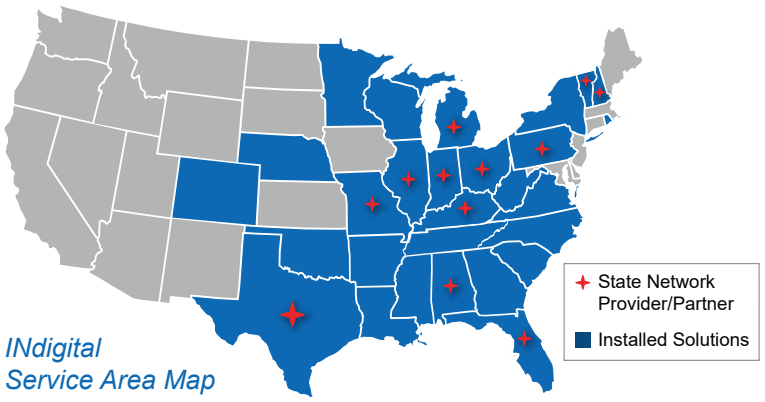
30+ years of connecting businesses, homes and rural areas with the fastest internet speeds available through self-healing fiber-optic networks.

INdigital

INdigital

Widely recognized as an industry leader and ESInet design/build/operate 9-1-1 system service provider. Additionally, INdigital has successfully created, delivered and operated many first-to-market and best-in-class Next Generation services.

The company has advanced to providing service in 12 states, equipping 500+ PSAPs, and serving a population of 32.6 million.



INdigital Service Area Map

Together, Hamilton and INdigital have developed several key advances in Next Generation core services and share the common goal of advancing the industry.

Hamilton and their team of experts provide trusted, reliable resources for Next Generation 9-1-1, as well as a customized, structured implementation approach that will offer PSAPs and states a number of advantages in technology and service delivery.

EXECUTIVE TEAM

Hamilton NG911 is committed to building trusted partnerships and providing quality services to the emergency response industry. Dedicated team members are here to help you transition to the future of 9-1-1. With a full team of technicians working behind the scenes to provide reliable service, these individuals are at the forefront of our operation.

John Nelson
President

Dan Molliconi
Chief Operating Officer

Dixie Ziegler
Chief Operating Officer, Hamilton Relay, Inc.

Gary Warren
Senior Consultant

Jim Ediger
Senior Regulatory Compliance Expert

Ryan Wineteer
Hamilton NG911 Manager

Jennifer Dennis
Executive Assistant

Jeff Knighton
Software Engineer

Seth Marks
Software Engineer

Wayne Hahn
Network Engineer

Marty Pierson
Network Data Center Engineer

Robert Leonard
Information Security Manager

Abby Magtoto
Outreach Account Specialist

170+
combined years of experience in 9-1-1 service and technology innovations.

SUMMARY

The Hamilton approach delivers multiple advantages in technology and service delivery. The expert and dedicated team at Hamilton delivers the essential tools necessary to provide all components for a fully functioning, integrated solution.

> *"Hamilton has been providing 9-1-1 service to our customers since its introduction in 1968. We have the resources to successfully implement the conversion to Next Generation 9-1-1."*
>
> *- **John Nelson**, Hamilton NG911 President*

A trusted solution and technical expertise.

- 51 years of delivering 9-1-1 service
- Robust telecommunications infrastructure
- Contracted telecommunications services on local, state and regional levels
- Wide range of regulatory experience
- Broad understanding of accessibility components

Through a long history of experience, Hamilton has proven the ability to coordinate and support projects of this size, confirming a unique position to be your Next Generation 9-1-1 solution provider.

HAMILTON NG911

CONTACT INFO

email:
NG911@hamiltontel.com

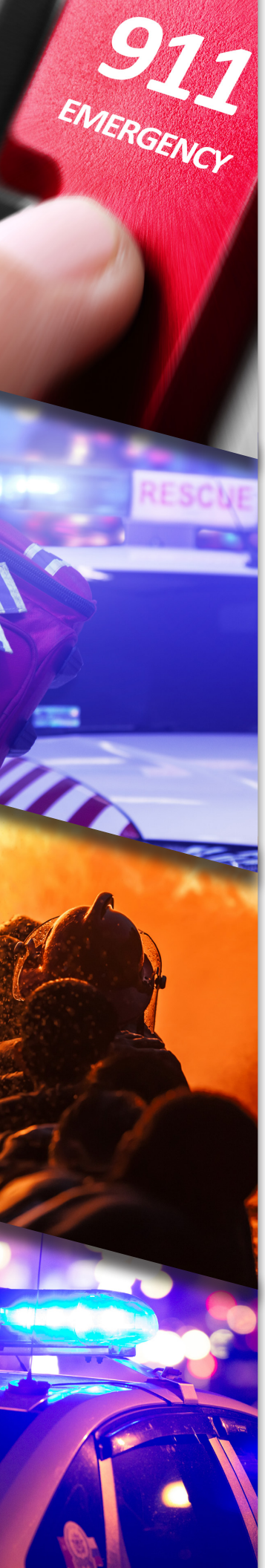
phone:
877.912.9461

website:
HamiltonNG911.com

Ask About Additional Resources:

- FCC Education Day Demo
- MEVO(+) Demo
- Cybersecurity Webinar
- RTT White Paper

Table of Contents



SECTION II:
TERMS AND CONDITIONS

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:
JN			

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:
JN			

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:
JW			

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:
JW			

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:
JW			

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:
JW			

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:
JW			

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:
JW			

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:
JN			

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:
JN			

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:
JN			Hamilton has received pre-qualification for the $500,000 bond request. Please see Appendix 1 – Hamilton NG911 Pre-Qualification Bond Letter.

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:
JN			

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:
JW			

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:
JW			

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:
JW			

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:
JN			

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

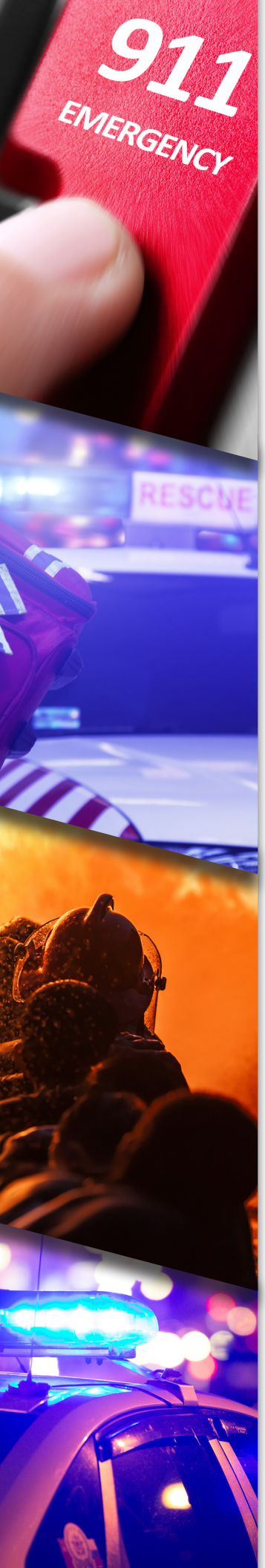
Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
JN			

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.



SECTION III:
CONTRACTOR DUTIES

III. CONTRACTOR DUTIES

A. INDEPENDENT CONTRACTOR / OBLIGATIONS

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

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:

1. Any and all pay, benefits, and employment taxes and/or other payroll withholding;
2. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;
3. Damages incurred by Contractor's employees within the scope of their duties under the contract;
4. 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;
5. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,
6. 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.

B. EMPLOYEE WORK ELIGIBILITY STATUS

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

		Solicitation Response (Initial)	
JM			

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:

1. 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.

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

3. 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.

4. 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.

C. 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.

D. COOPERATION WITH OTHER CONTRACTORS

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

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.

E. PERMITS, REGULATIONS, LAWS

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

JW			

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.

F. OWNERSHIP OF INFORMATION AND DATA / DELIVERABLES

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

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.

G. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
JW			Hamilton's insurance year coincides with the fiscal year and current coverage will renew July 1, 2020. Hamilton has included a COI for the current year as Appendix 2 – Certificate of Insurance/Acord Form (COI).

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:

1. Provide equivalent insurance for each subcontractor and provide a COI verifying the coverage for the subcontractor;
2. 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,
3. 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.

2. **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."	

3. 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.

4. 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.

H. ANTITRUST

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

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.

I. CONFLICT OF INTEREST

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

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.

J. STATE PROPERTY

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

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.

K. SITE RULES AND REGULATIONS

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

JN			

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.

L. ADVERTISING

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

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.

M. 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.

N. DISASTER RECOVERY/BACK UP PLAN

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

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.

O. DRUG POLICY

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

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.

P. WARRANTY

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

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.

SECTION IV: PAYMENT

IV. PAYMENT

A. 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."

B. 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

C. INVOICES

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

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.

D. INSPECTION AND APPROVAL

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

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.

E. 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.

F. 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).

G. 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.

H. 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:
JM			

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.

V. PROJECT DESCRIPTION AND SCOPE OF WORK

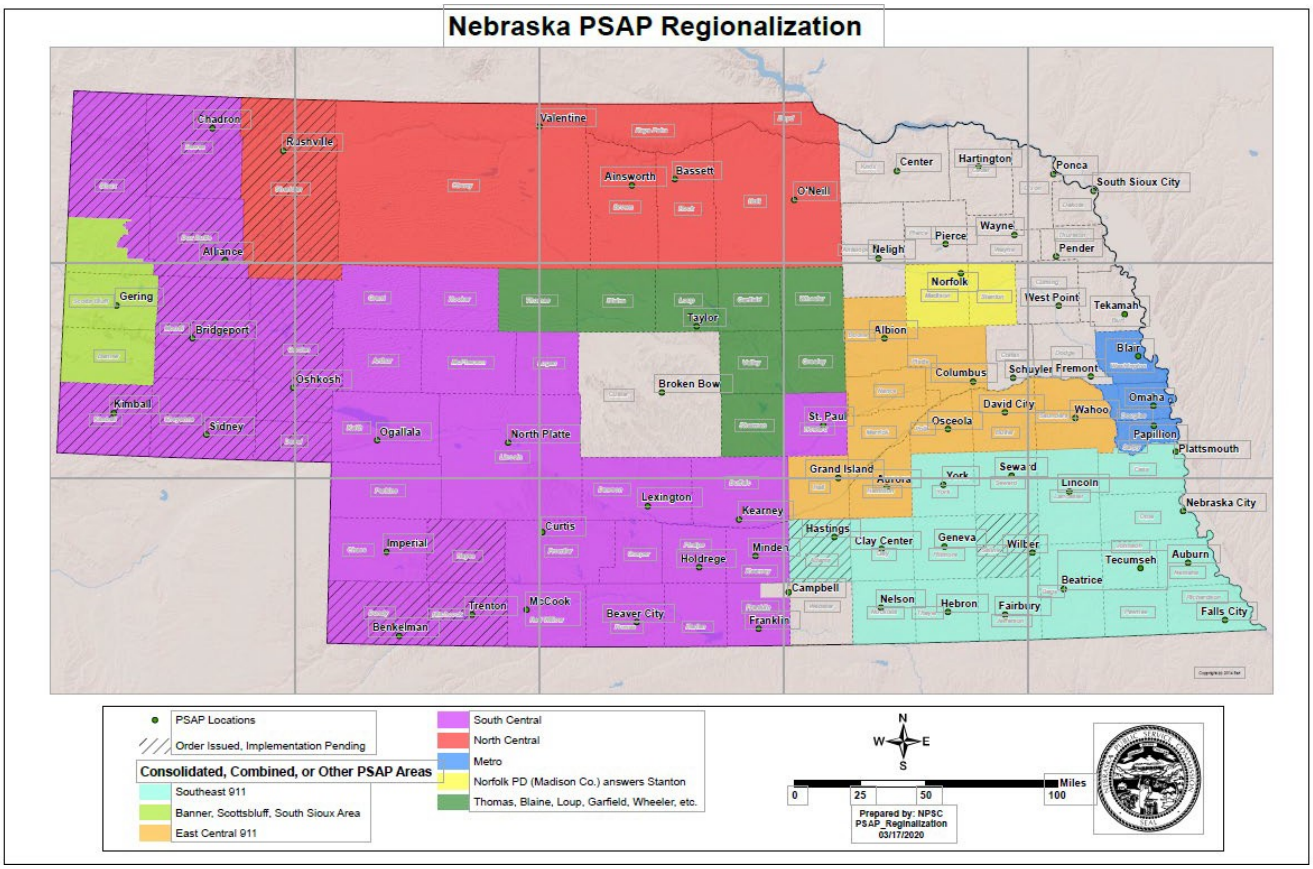
A. Background and Project Scope

The Nebraska Public Service Commission, State 911 Department (The Commission) is the statewide authority responsible for implementing and coordinating 911 service in the state. The Commission is seeking proposals for a statewide ESInet and NGCS to help advance Next Generation 911 (NG911) across the state.

Today, the local PSAPs manage and maintain independent relationships with 911 service provider and network providers. With this procurement, the Commission will establish and support a statewide ESInet and NGCS to provide 911 service to the regions throughout the state.

The state has 68 PSAPs that take approximately 1.13 million calls a year and serve a statewide population of 1.929 million people. The largest population centers are Douglas County (566,880) and Lancaster County (317,272). Many of the PSAPs throughout the state have joined together to form regions. Each region utilizes call-handling equipment (CHE) that operates in a host/remote configuration. The Commission is looking for the statewide ESInet to include physically redundant connections into each of the regional host systems. The current regional configuration is depicted in the diagram (Figure 1) below; however, it is anticipated that over the next 12 to 18 months, additional PSAPs will join one of the different regions or a new region may be formed. Updated regional information can be found on the Public Service Commission's website at www.psc.nebraska.gov.

FIGURE 1



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

B. Composition of the Request for Proposal

This RFP is composed of two elements: Emergency Services Internet Protocol [IP] Network (ESInet) and Next Generation Core Services (NGCS). Bidders may respond to a single element (Option A- ESInet or Option B - NGCS) or both elements (Option C – ESInet and NGCS. The State will evaluate all conforming proposals. A highest scoring bidder will be identified for each of the options (A, B, and C) The State reserved the right to award any and all options at its sole discretion.

The statewide NG911 initiative will focus on two primary areas, the ESInet and NGCS.

1. Option A: Deployment of an ESInet

With the deployment of a statewide ESInet, the Commission is seeking a solution that connects each regional host to the statewide ESInet. Key project elements for ESInet deployment include, but are not limited to:

- **a.** Deployment of a public safety-grade network that is monitored and managed to ensure security, reliability and high availability;
- **b.** Implementation of a network that is affordable and provides a consistent level of service to all PSAPs throughout the state;
- **c.** Development of a phased implementation approach that minimizes service impact to PSAP operations; and,
- **d.** Cooperation and coordination with the NGCS provider throughout and after implementation.

2. Option B: Deployment of Next Generation Core Services (NGCS)

The Commission is seeking an NG911 call-delivery system that provides highly available call routing and delivery to the regional end points throughout the state. Key project elements for NGCS deployment include but are not limited to:

- **a.** Deployment of monitored and managed core services that are redundant, resilient, sustainable, and provide an upgrade path to new technologies as NG911 services evolve;
- **b.** Transition to the use of Geographic Information System (GIS) data for geospatial call routing;
- **c.** Planned transition timelines that limit the overlap between the legacy selective router network and NGCS; and,
- **d.** The ability to support various types of requests for assistance including calls, text messages, video messages, additional data, etc.

3. Option C: Deployment of an ESInet and NGCS

Includes all requirements of both Option A and Option B.

Please note that proposals may be submitted for all of the desired services or a portion of the services based on Bidder capabilities. For example, a network provider may bid only the ESInet portion of the proposal and not the NGCS.

The Commission's intent is to release an RFP soon after the release of the ESInet/NGCS RFP that addresses the connectivity from the host locations to the regional PSAP locations.

C. Bidder Requirements:

1. Bidders should include with their response:
   - **a.** Configuration Solution – A diagram showing the major components (hardware, software, and network layout) for the proposed system, accompanied by tables containing short descriptions of the diagrammed components in terms of their value or benefit to the Commission and the Public Safety Answering Points (PSAPs).
   - **b.** Attachments – Cost Proposal, with a detailed description of its firm fixed pricing.
   - **c.** Appendices – The Bidder may include appendices and reference them from within the proposal response. This is particularly appropriate for lengthy responses on a single subject. Understanding the intent of the Bidder shall be possible without the reading of the appendices.
   - **d.** Brochures – Hardware, software, or service brochures may be submitted with response where appropriate.

D. General Requirements – Technical

1. General requirements – Commission Requirements

a. Industry Standards

The Commission seeks a standards-based solution that complies with nationally accepted standards and requirements applicable to ESInet architecture, security, and interface functionality. All aspects of the Bidder's proposed system design, deployment, operation, and security shall be in full compliance with the standards, requirements, and recommendations located in the 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)

Table 1: Adopted Standards

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
ATIS	ATIS-0500017	Considerations for an Emergency Services Next Generation Network (ES-NGN)	Identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next-generation telecommunications networks.	Version 1 June 2009
DOJ	CJISD-ITS-DOC-08140-5.6	Criminal Justice Information Services (CJIS) Security Policy	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information.	Version 5.6 June 5, 2017
IETF	RFC 3261	SIP: Session Initiation Protocol	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	Version 1 July 7, 2002
IETF	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Defines the generic URI syntax and a process for resolving URI references, along with guidelines and security considerations for the use of URIs on the Internet.	Version 1 January 2005
NENA/ APCO	REQ-001.1.2-2018	Next Generation 911 PSAP Requirements	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP.	Version 1.2 April 5, 2018
NENA/ APCO	INF-005	Emergency Incident Data Document (EIDD) Information Document	Provides a recommended list of data components, their relationships to each other, the data elements contained within each data component, and the registries that control the available values for appropriate data elements. Initiates the process to create a National Information Exchange Model (NIEM).	February 21, 2014 Scheduled to be replaced by a standards document
NENA	STA-015.10-2018	Standard Data Formats for 911 Data Exchange & GIS Mapping	Establishes standard formats for Automatic Location Identification (ALI) data exchange between service providers and Database Management System (DBMS) providers, a GIS data model, a data dictionary, and formats for	Version 10 August 12, 2018

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
			data exchange between the ALI database and PSAP controller equipment.	
NENA	STA-008.2-2014	Registry System Standard	Describes how registries (lists of values used in NG911 functional element standards) are created and maintained.	Version 2 October 6, 2014
NENA	STA-010.2-2016	Detailed Functional and Interface Specifications for the NENA i3 Solution	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards.	Version 2 September 10, 2016
NENA	INF-016.2-2018	Emergency Services IP Network Design for NG911 (ESIND)	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInet.	Version 1 April 5, 2018
NENA	75-001	Security for Next Generation 911 (NG-SEC)	Establishes the minimal guidelines and requirements for levels of security applicable to NG911 entities.	Version 1 February 6, 2010
NENA	INF-015.1-2016	NG911 Security Information Document	Provides mechanisms and best practices for cybersecurity for i3 systems	Version 1 December 8, 2016
NERC	CIP 002-CIP 009	Critical Infrastructure Protection	Addresses the security of cyber assets essential to the reliable operation of the nation's critical infrastructure.	Version 1 December 16, 2009
NIST	FIPS 140-33	Security Requirements for Cryptographic Modules	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information.	Version 2 March 22, 2019
NIST	Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure.	Version 1.1 April 16, 2018
TIA	TIA-942-A	Telecommunications Infrastructure Standard for Data Centers	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers.	Revision A March 2014

As industry standards evolve, the Bidder's solution shall be upgraded to maintain compliance with the current version of established industry standards. The Bidder's solution shall support new ESInet, NGCS and security industry standards within 18 months of ratification of applicable industry standards at no additional cost to the State. Compliance requirements apply also to the supporting standards referenced within each standard. As solution updates are made to maintain compliance, the solution shall not abandon services or feature functionality in place at the time of the solution upgrade. The Bidder shall uncover any performance or feature changes prior to the upgrade and report them to the Commission for approval.

b. Public Safety-Grade Definition

The national standards listed in this document provide standards and requirements an IP network and core functions shall meet or exceed to be considered an ESInet. 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) or accepted by the public safety community. For the purpose of the requirements associated with this ESInet and NGCS design and deployment, the following metric is used to define public safety-grade:

i. Reliability:

"Reliability" is the ability of a system or component to perform the required functions under stated conditions for a specified period of time. The traditional measure of system or component reliability is Mean Time Between Failure (MTBF). The required MTBF must result in system reliability of 0.99999 as recommended in NENA-INF-016.2-2018, Section 2.10.1.

ii. Availability:
"Availability" is the degree to which a system or component is operational and accessible when required for use. System availability is dependent upon the Mean Time to Repair (MTTR) calculation, which measures the time it takes to recover from component failure, a failed system upgrade, operator error, or other scheduled and unscheduled system interruption. Downtime must not exceed five (5) minutes per year, or 99.999 percent availability, as recommended in NENA-INF-016.2-2018, Section 2.10.1.

iii. Security:
Secure communications must be retained through the following measures, as recommended in NENA-INF-015.1-2016, Section 3.2:

- **a)** Rivest–Shamir–Adleman (RSA)-based public-key cryptography using X.509 certificates to authenticate elements, agencies, and agents. Mutual authentication must exist between both ends of a communication.
- **b)** An eXtensible Access Control Markup Language (XACML)-based Data Rights Management (DRM) system to control authorization.
- **c)** Advanced Encryption Standards (AES) based encryption to provide confidentiality.
- **d)** Secure Hash Algorithm (SHA)-based digest-based digital hashing to provide integrity protection.
- **e)** Dsig-based digital signatures to provide non-repudiation.

iv. Network Traffic Restrictions:

The established metrics in this definition can be achieved through system and component redundancy, diversity, resiliency, and other similar engineering methodologies. When the term "public safety-grade" is applied in this document, the Bidder shall describe how bidder's network and core service system and components for critical functions either meets or exceeds the standards-based, public safety-grade definition .

When this term is used in this document to describe the required level of service for the ESInet, and NGCS, functionality, the Bidder shall confirm that its service and components meet or exceed both the national standards listed in Table1 and the public safety-grade definition.

SECTION VI:
CORPORATE OVERVIEW

VI. PROPOSAL INSTRUCTIONS

This section documents the requirements that should be met by bidders in preparing the Technical and Cost Proposal. Bidders should identify the subdivisions of "Project Description and Scope of Work" clearly in their proposals; failure to do so may result in disqualification. Failure to respond to a specific requirement may be the basis for elimination from consideration during the State's comparative evaluation.

Proposals are due by the date and time shown in the Schedule of Events. Content requirements for the Corporate Overview, Technical and Cost Proposal are presented separately in the following subdivisions, format and order:

A. PROPOSAL SUBMISSION

1. CORPORATE OVERVIEW

The Corporate Overview section of the Technical Proposal should consist of the following subdivisions:

a. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

Hamilton NG911, Inc. (d/b/a Hamilton) is a Nebraska Corporation and was organized to do business in 2017. Hamilton is a service provider in the Next Generation 9-1-1 (NG 9-1-1) emergency communications marketplace. Hamilton NG911, Inc. (d/b/a Hamilton) is a division of Hamilton Telecommunications (parent company is Nedelco, Inc.,) a diversified communications and technology services provider headquartered at 1006 12th Street, Aurora, Nebraska, 68818. Hamilton NG911's name and form of organization has not changed since first organized in 2017. Originally founded in 1901 as an independent local exchange carrier in central Nebraska, today Hamilton encompasses eight primary company divisions that allow Hamilton to operate on a local, regional, and national basis.

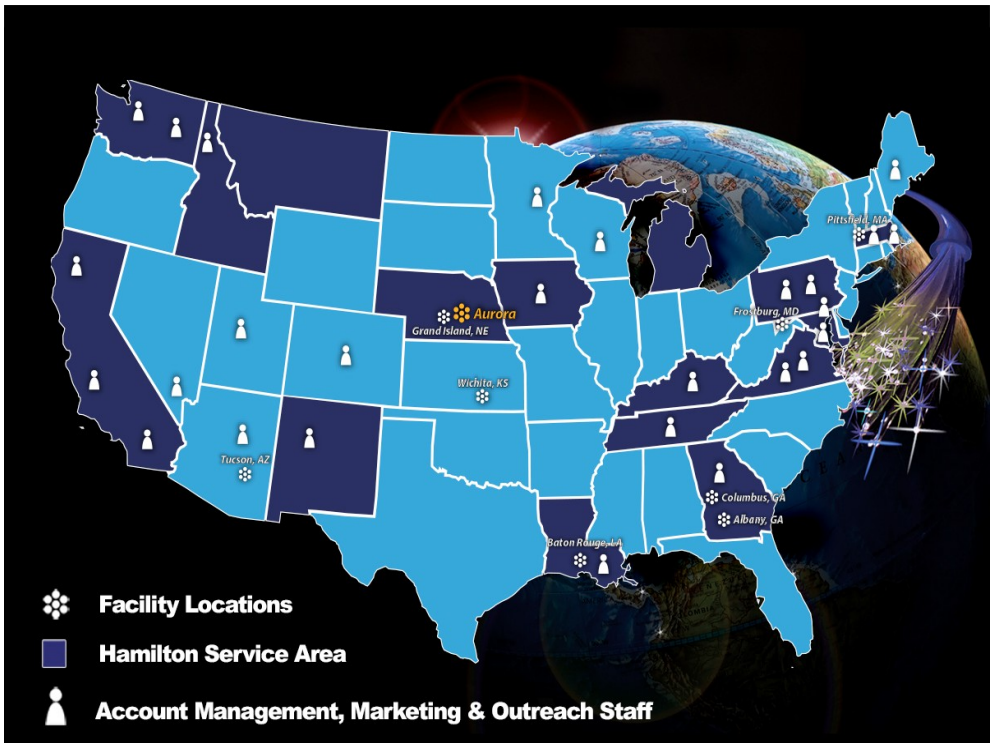
Hamilton offers a wide variety of telecommunications and technology services. Below, Hamilton has provided some examples of service offerings provided by several of its company divisions:

- Hamilton Relay: Provides contracted Traditional Relay (711 service) and Captioned Telephone services through 21 contracts to 15 states, the District of Columbia, and the Island of Saipan, and is a provider of Internet-based Captioned Telephone service nationwide. Currently, Hamilton Relay is the only relay provider, and possibly the only telecommunications company, leading multiple native Real-Time Text (RTT) pilot projects across the United States. Hamilton Relay has provided text access for hard of hearing and deaf individuals utilizing IP based technologies and has provided relay service on thousands of calls to 9-1-1 services.
- Hamilton Telephone Company: Provides fiber to the home to thousands of Nebraska residents and businesses utilizing an IP-based softswitch and has provided local area trunks for 9-1-1 services within its service territory since the beginning of 911 services.
- Hamilton.net: Provides gigabit capable internet services to customers within the Hamilton Exchange, Wireless internet service to thousands of rural subscribers, and core network management and bandwidth connectivity for other businesses and several of Nebraska ILECs and ISPs utilizing its extensive in-house resource of IP engineers and its redundant 40 Gbps internet access connections to the cloud.
- Hamilton Long Distance: A certified Nebraska CLEC, provides traditional long distance, business class fiber connectivity and data transport services, and is a certified nomadic VoIP provider in all 50 states. Hamilton Long Distance manages a robust. redundant, and critical fiber-based network serving seven relay center locations and multiple business locations nationwide.
- Hamilton Information Systems: Provides business to business network management and cyber security services, business phone systems, access control and security solutions, and data center services and cloud IT to businesses across the country.
- Hamilton Innovations: Provides innovation services for Hamilton business lines and beyond. Hamilton Innovations is responsible for creating smart communication solutions for companies to stay connected and for further evolving Hamilton's products, services, and solutions. Hamilton Innovation has developed Real-Time Text (RTT) and text-to-9-1-1 related technologies, leading the industry in this area, and has participated in many NENA Industry Collaboration Events (ICE).
- Nedelco Shared Services: An organization of highly skilled individuals in all facets of business – network and switching management, security, LAN management, software development, project and product management, enterprise software management, finance and accounting, sales and marketing, and human resources. This group of professionals provide the necessary resources to support Hamilton NG911.

As referenced on several occasions above, elements of Hamilton's 9-1-1 business line have existed in other Hamilton company divisions for many, many years. prior to the formation of Hamilton NG911. For example, Hamilton Telephone Company has provided certain elements of 9-1-1 in the local region throughout its 100+ year history and Hamilton Relay has provided 9-1-1 service for its relay customers for the past 30 years through its relay service division. In 2017, it was decided that Hamilton would designate a separate, distinct, and dedicated subsidiary to providing 9-1-1 services as a result of Hamilton's vast experience providing so many elements of NG 9-1-1 services. In addition, Hamilton is able to fully carry out its mission of providing the latest in telecommunication technologies as Hamilton works in its home state to ensure the citizens of Nebraska are able to take full advantage of NG 9-1-1.

To further assess the economic impact of Hamilton NG911 services and solution on the state of Nebraska, Hamilton had an economic impact study completed by Ernie Goss of Goss & Associates Economic Solutions. Mr. Goss' analysis concluded that selecting Hamilton NG911 as the state's NG 9-1-1 provider would have a positive impact on the local and state economies, state and local tax collections, and the state's labor force. For example, it was concluded, based on a hypothetical contract of five million dollars for NG 9-1-1 services, that the operation will generate, on an annual basis, $9,403,539 in total economic impact: $4,178,457 in wage and salaries and $421,743 in self-employment income for the state of Nebraska. In addition, it is estimated that this five-million-dollar contract will produce $354,779 in state and local taxes. According to the study, these economic impacts are nearly double the resulting impacts achieved by out-of-state competitors. Additionally, for year one, Hamilton NG11 operations would support 146 jobs in the economy with a total payroll of approximately $4,178,457 compared to a much lower 102 jobs with a total payroll of $2,760,016 for out-of-state competitors. Overall, Hamilton is invested in the state of Nebraska and wants to continue this investment in the state's communities by providing professional employment opportunities for local citizens and the means for continued support of our local economies. To review the full economic impact study, please see Appendix 3 – The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska.

Hamilton will deliver the robust NG 9-1-1 services desired in Nebraska. As a result of Hamilton's deep history, experiences and knowledge of 9-1-1 and NG 9-1-1 services, 118-year history of managing telecommunications infrastructure, experience in contracted telecommunications services on state and local levels, a wide range of regulatory experience, and a broad understanding of accessibility components, Hamilton NG911 is uniquely qualified to be the chosen Bidder to implement a standards-compliant Emergency Services IP Network (ESInet) along with Next Generation Core Services (NGCS) for the state of Nebraska.



It is important to note that Hamilton's proposed solution adheres to all nationally accepted standards and requirements applicable to system design, deployment, operation and security as specified in Table 1: Adopted Standards and will ensure compliance with standards through the course of the contract, as collaboration will occur at all stages, including design development and approval, as well as thorough testing and acceptance procedures.

For example, the Security for Next Generation 9-1-1 Standard (NG-SEC) 75-001 identifies the basic minimum security requirements and guidelines applicable to NG 9-1-1 entities, providing a basis for assessing levels of security and risk, completing security audits, and exception approval/risk acceptance process in the case of non-compliance with these guidelines. Hamilton takes a holistic approach not only following the NG-SEC policies, but also the National Institute of Standards and Technology (NIST) framework. Hamilton utilizes the NIST Special Publication 800-53 procedures to evaluate network inventory to then create security controls and associated procedures based on the levels of risk associated with the identified threat vectors.

Furthermore, the Hamilton information security team boasts a CompTIA Security+ certification and carries network management experience in private and public sectors, as well as in a number of statewide government contracts across the county. This is one of many examples where Hamilton's body of work not only adheres to standards, but exceeds them. In addition, all equipment provided in this response complies with the Federal Communications Commission (FCC) rules Part 15, Class A. Additionally, all equipment provided is non-proprietary and commonly available from a wide variety of leading manufacturers.

Hamilton's additional wealth of experience developing solutions that meet accessibility and communication needs aid in its ability to meet the qualifications for the performance of the potential contract. With 29 years of success in the telecommunications relay services industry, Hamilton offers a diverse level of technical knowledge and skill managing circuits and voice traffic across the country.

Hamilton has deep-seeded roots in the telecommunications industry, bringing significant competency in data solutions, including hardware installation and maintenance.

Additionally, Hamilton owns and operates two geographically diverse data centers in Nebraska and is well versed in maintaining 99.999% uptime in mission critical operations. Hamilton has also been at the forefront of the cybersecurity conversation with the National Telephone Co-operative Association (NTCA), the National Emergency Number Association (NENA) and Association of Public-Safety Communications Officials (APCO).

In addition to its cybersecurity contributions, Hamilton's industry association participation extends nationwide and into many state NENA and/or APCO chapters. For example, Hamilton proudly supports the Nebraska APCO/NENA Chapter and a member of Hamilton's staff, Jennifer Dennis, currently serves on the Educational Committee for the 2020 NE NENA/APCO Conference. This is one example of many where Hamilton has been involved to help carry out NENA's mission to promote research, planning, training and education within our state and beyond.

The Hamilton family of companies currently employs over 1,000 individuals nationwide and is committed to delivering the latest in telecommunications and technology services, along with personalized and trusted customer support. With over 118 years of diverse experience in the industry, Hamilton is uniquely qualified to operate at the highest level of emergency service standards.

To fulfill the requirements of the contract, Hamilton staff will be working from the following data center facility locations:

Nebraska Data Center (NDC) – 1623 Farnam St., Omaha, NE 68102

Hamilton Data Center – 1006 12th St. Aurora, NE 68818

As detailed throughout this proposal, Hamilton has a vast amount of corporate experience relevant to this project. Select government contracts for Hamilton are highlighted in the chart below verifying Hamilton has a proven track record of managing comparably sized projects and responding to the needs of our customers, state regulatory bodies, and other industry related organizations in an effective and efficient manner.

NUMBER	CONTRACT PERIOD	ENTITY	DESCRIPTION	CONTACT
10-11160	**12/2/15 – Present**	**California**	Hamilton - Captioned Telephone and Traditional Relay Service provider since 2010. Sole provider of services since 2015.	Brent Jolley Interim State of California TRS Administrator California Public Utilities Commission 505 Van Ness Ave. Third Floor San Francisco, CA 94102 Email: Brent.Jolley@cpuc.ca.gov
CTS 08-11010 **TRS 04-10463**	**10/24/17 – Present**	**District of Columbia**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2014.	Kirsten Williams, Esq. Deputy Executive Director, DC Public Service Public Service Commission of the District of Columbia 1325 G Street N.W. Suite 800 Washington, DC 20005 Phone: (202) 626-0200 Email: kwilliams@psc.dc.gov
05-10618	**4/1/16 – Present**	**Georgia**	Hamilton - Traditional Relay Service provider since 2006 and Captioned Telephone provider since 2008.	Tonika Starks Contract Administrator, Georgia Relay Georgia Public Service Commission Service 244 Washington Street, SW Atlanta, Georgia 30334-5701 Voice: (404) 657-4990 Email: tstarks@psc.state.ga.us

96-10042	**12/1/16 – Present**	**Idaho**	Hamilton - Traditional Relay Service provider since 1992 and Captioned Telephone provider since 2006.	Kelli Toohill Idaho TRS Administrator PO Box 351 Lynden, WA 98264 Voice/Fax: (604) 652-0447 Email: idahorelay@gmail.com
CTS 06-10726 **TRS 04-10534**	**1/1/17 – Present**	**Iowa**	Hamilton - Traditional Relay Service provider since 2005 and Captioned Telephone provider since 2007.	Kelsey Seaberg Project Manager, Relay Iowa 1375 E. Court Des Moines, IA 50319 515-725-7367 Email: Kelsey.Seaberg@iub.iowa.gov
99-10040	**5/16/16 – Present**	**Commonwealth of Kentucky**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2016.	Jim Stevens Contract Administrator, Kentucky Relay Kentucky Public Service Commission 211 Sower Boulevard P.O. Box 615 Frankfort, KY 40602 Phone: 502-564-3940 Email: jim.stevens@ky.gov

97-10035	**1/15/17 – Present**	**Louisiana**	Hamilton - Traditional Relay Service provider since 1998 and Captioned Telephone provider since 2009.	Ted Hankins President, Louisiana Relay Administration Board 100 CenturyLink Drive Monroe, LA 71203 Phone: 318-388-9416 Cell: 318-235-5400 Email: ted.hankins@centurylink.com
07-10803	**3/1/20 – Present**	**Maryland**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2007.	David Bahar Project Manager, Maryland Relay 301 West Preston Street, Suite 1008A Baltimore, MD 21201 Video Phone: (443) 842-7590 Email: david.bahar@maryland.gov
13-11538	**7/1/18 – Present (April here not sure this matters but I have 8/1/18)**	**Commonwealth of Massachusetts**	Hamilton - Traditional Relay Service provider since 2008 and Captioned Telephone provider since 2010.	Monna Wallace Massachusetts Relay Administrator Director of Programs, Massachusetts State 911 Department 151 Campanelli Drive, Suite A Middleborough, MA 02346 Phone: 508-828-2911 Email: monna.wallace@state.ma.us

TAM 15-11685 **AT&T 15-11715**	**12/19/14 – Present** **2/1/15 – Present**	**Michigan**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2015.	Scott Stevenson President, Telecommunications Association of Michigan Phone: (517) 482-1258 Website: www.telecommich.org
06-10643	**2/28/16 – Present**	**Montana**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2006.	Mary Taylor State Contract Manager/Project Manager MTAP Executive Director PO Box 4210 Helena, MT 59604 Voice: (406) 444-4290 Email: mary.taylor@mt.gov
09-11093	**7/1/18 – Present**	**New Mexico**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2009.	Nathan Gomme Relay Administrator, State of New Mexico New Mexico Commission for Deaf & Hard of Hearing 505 Marquette Ave NW Albuquerque, NM 87102 VP: (505) 435-9319 Email: nathan.gomme@state.nm.us

CTS 07-10760 **TRS 15-11720**	**12/16/14 – Present**	**Commonwealth of Pennsylvania**	Hamilton - Traditional Relay Service provider since 2014 and Captioned Telephone provider since 2007.	Eric Jeschke Contract Administrator, Pennsylvania Relay Pennsylvania Public Utility Commission 400 North Street Keystone Building Harrisburg, PA 17120 Phone: (717) 783-3850 Email: ejeschke@state.pa.us
04-10529	**10/1/06 – Present**	**Saipan**	Hamilton - Traditional Relay Service provider since 2004.	Rob Harrell Micronesian Telecommunications Corporation (d/b/a the PTI) P.O. Box 500306 Saipan, MP 96950 Phone: (670) 682-2614 Email: rob.harrell@itehq.net
10-11217	**11/1/2015 – Present** **(April here, I have 9/1/2015)**	**Tennessee**	Hamilton - Captioned Telephone provider since 2010.	Monique Brazelton Contract Administrator, Tennessee CapTel Tennessee Regulatory Authority 502 Deaderick Street, 4th Floor Nashville, TN 37243 Phone: (615) 741-2904 Email: Monique.Brazelton@tn.gov

CRS 11-11279 **TRS 16-11819**	**7/31/15 – Present**	**Commonwealth of Virginia**	Hamilton - Captioned Telephone service provider since 2011 and Traditional Relay Service provider since 2015.	Doug Leslie Strategic Sourcing Consultant Supply Chain Management Virginia Information Technologie s Agency (VITA) 11751 Meadowville Lane Chester, Virginia 23836-6315 Phone: (804) 416-6161 Email: doug.leslie@vita.virginia.gov
15-11748	**7/1/15 – Present**	**Washington**	Hamilton - Traditional Relay Service and Captioned Telephone provider since 2015.	Steven Peck ODHH TRS Contract Administrator Department of Social and Health Services 4450 10th Ave SE, Lacey, WA 98503 PO Box 45301, Olympia, WA 98504 Phone: (360) 339-7762 Email: pecksc@dshs.wa.gov

b. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that proposal evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

The State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

Hamilton has provided the requested financial information, including a bank reference, and seeks to submit this information confidential and withheld from the public pursuant to applicable Nebraska law, including but not limited to *Neb. Rev. Stat.* Section 84-712.05(3). Hamilton's Financial Overview document demonstrates Hamilton's financial stability proving Hamilton's ability to fulfill all financial obligations of the Contract. Please see Appendix 4 – Hamilton Financial Overview (PROPRIETARY INFORMATION).

In addition, Hamilton NG911, Inc. has no pending litigation and has no history of litigation in the past 10 years. Hamilton NG911, Inc.'s parent company, Nedelco, Inc., and its affiliates, have no material pending litigation against it that would adversely affect its ability to meet contract requirements pursuant to this RFP.

Hamilton understands the State may elect to utilize a third party to conduct credit checks as part of the corporate overview evaluation. Hamilton will willingly comply and collaborate with the State during credit checks as necessary.

c. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the proposal due date, the bidder should describe the circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded bidder(s) will require notification to the State.

Hamilton does not anticipate any change in ownership or control of the company during the coming twelve (12) months following the proposal due date and acknowledges the notification requirement listed above.

d. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

The following Hamilton office location will be responsible for the Bidder's performance pursuant to an award of a contract with the State of Nebraska:

- Hamilton NG911 – 1006 12th Street, Aurora, NE 68818

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous five (5 years). If the organization, its predecessor, or any Party named in the bidder's proposal response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

Hamilton NG911, Inc. has not had any dealings with the State over the previous five (5) years. However, several of Hamilton's sister companies have had, and continue to have, contracts with the State. These contracts include:

- Hamilton Long Distance is under contract with the State of Nebraska Office of the CIO/Service Agreement for Ethernet transport service – NDOR to College Park dated June 7, 2010. Under that Master Service Agreement, the following Addendums/Service Orders have been authorized:
  - Addendum 1: dated July 11, 2011 adding Giltner to College Park
  - Addendum 2: dated August 26, 2013 amending Giltner to College Park (Contract: 201005-206)
  - Addendum 3: dated February 27, 2014 amending Giltner to College Park and replacing Addendum 1 (State Order #013022414-01)
  - Addendum 4: dated May 22, 2015 adding Nebraska State Patrol (Nebraska Law Enforcement Training Center) DIA services (State Order #013052015-02)
  - Addendum 4.1: dated July 1, 2015 adding a circuit for Nebraska State Patrol (Nebraska Law Enforcement Training Center) (State Order #013052015-02)
  - Addendum 5: dated August 6, 2015 modifying Addendum 4.1 (State Order #013062615-01)
  - Addendum 6: dated August 6, 2015 adding NDOR-Seward to College Park (State Order #013063015-01)
  - Addendum (not numbered): dated May 3, 2017 upgrading circuit for NDOR-Aurora (State Order #013050317-01)
  - Service Order for Install: dated January 8, 2019 adding point to point circuit between College Park and Hamilton Co Courthouse for 48 months (State Order #103010819-01)
  - Service Order Agreement Renewal: dated February 18, 2020 renewing contract for 48 months for circuit ID EOF-7, NETV (State Order #103021820-01)
- Hamilton.net entered into a contract with the State of Nebraska CIO's Office-Hamilton County Automation/DSL Service Agreement dated September 17, 2010 (State Order #: 013122205-01)
  - Service was upgraded on March 8, 2018 (State Contract #013030818-01) and terminated on 8/30/2019.
- Hamilton.net is under contract with the State of Nebraska CIO's Office-State Patrol Aurora/DSL Service Agreement dated September 17, 2010 (State Order #: 013092704-02)
- The State of Nebraska facilitated RFPs for Service Contract/Agreements for Circuits in 2013, 2018, and 2020. Hamilton Long Distance is currently under contract with Aurora, Central City, Doniphan-Trumbull, Giltner, and Hampton to fulfill the agreements.

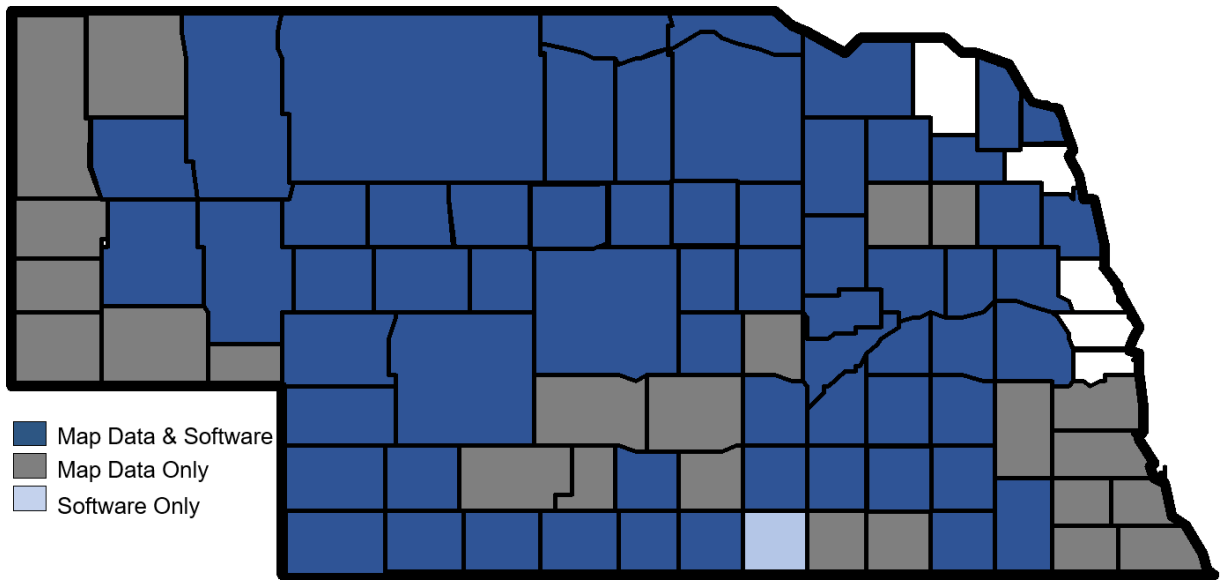
In addition, Hamilton Telephone Company and Hamilton Long Distance are certificated carriers pursuant to orders of the Nebraska Public Service Commission.

Hamilton provides local telephone services to various State agencies which have offices in Hamilton's local telephone service area. Hamilton continues to review, and respond, to Requests for Proposals from the State of Nebraska when the service requested include services customarily provided by Hamilton.

In addition, NebraskaLink has had, and continues to have, contracts with the State. These contracts include:

Contract Number	Original Bid Document	Dates
70992 04	5153 Z1 5761 Z1	03/28/2016 - 06/30/2020 07/01/2018 - 06/30/2022
51022 04	3827 Z1	07/01/2017 - 06/30/2018
76679 04	5562 Z1	05/10/2017 - 06/30/2020
89977 04	6206 Z1	04/20/2020 - 06/30/2024
51441 04		07/01/2017-06/30/2018
85542 04	6004 Z1	03/19/2019-06/30/2023

GeoComm has been doing business with Nebraska PSAPs for 25 years. GeoComm has active contracts for GIS data maintenance services, GIS Data Hub for data quality control, error checks, reporting, and regional aggregation, as well as software support agreements for PSAP mapping software applications. The map below depicts all the counties GeoComm currently has contracts with differentiated by color:



INdigital nor DDTI have had any contracts with the state over the previous five (5) years.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's proposal response is or was an employee of the State within the past five (5) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

If any employee of any agency of the State of Nebraska is employed by the bidder or is a subcontractor to the bidder, as of the due date for proposal submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist,

the bidder may be disqualified from further consideration in this proposal. If no such relationship exists, so declare.

Hamilton has reviewed its list of new hires within Nebraska for the past five (5) months. Hamilton does not have any new hires within this timeframe who have identified previous employment with the state of Nebraska. This statement is also true for Hamilton's subcontractors, INdigital, GeoComm, DDTI, and NebraskaLink. In addition, as of the due date for proposal submission, Hamilton and its subcontractors do not have any employees who are also employed by any agency of the state of Nebraska.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past five (5) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past five (5)) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's proposal accordingly. If no such termination for default has been experienced by the bidder in the past five (5) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

Neither Hamilton nor its subcontractors have had a contract terminated for default or non-performance within the past five (5) years.

h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the previous projects similar to this solicitation in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the proposal.

The bidder should address the following:

v. Provide narrative descriptions to highlight the similarities between the bidder's experience and this solicitation. Provide the number of ESInet and NGCS solutions implemented by the bidder that are in production today and lessons learned throughout the project that will be applied to the deployment of the Nebraska ESInet and NGCS solution. These descriptions should include:

a) The time period of the project;
b) The scheduled and actual completion dates;
c) The bidder's responsibilities;
d) For reference purposes, contracting entity name, contact name, contact title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.); and
e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

The following summary matrix provides an overview of projects similar to Nebraska's NG 9-1-1 solicitation in size, scope, and complexity. Further narrative descriptions of each project are provided below the summary matrix.

NUMBER	CONTRACT PERIOD	ENTITY	DESCRIPTION	CONTACT

IN911 Contract	**2005 – Present** **Milestones: 2007, 2010, 2012, 2015 & 2019**	**Indiana**	The IN911 network was completed by INdigital as the prime contractor. Over the 15-year life of the network, all work has been completed as scheduled and within the proposed budget. Currently, IN911 network is operated at a cost of approximately $11 million annually.	Ed Reuter State of Indiana Executive Director Phone: 317-234-8362 Email: ereuter@in911.net
Peninsula Fiber Network	**2014 - Present**	**Michigan**	INdigital has delivered NGCS services as a subcontractor to PFN for more than five years. Today, the annual budget for these services is in excess of $7 million. Due to the ad hoc nature of the network, it is difficult to define each due date. However, INdigital has worked diligently with PFN for more than five years to ensure the highest level of service to both PFN and the PSAPs of the state of Michigan.	David McCartney Peninsula Fiber Network, General Manager Phone: 906-226-2010 Email: gm@pfnllc.net

ANGEN Contract	**2016 – Present**	**Alabama**	A prime contract valued at approximately $52M was signed between INdigital and the Alabama 911 Board in 2016. Since then, INdigital has taken over the existing network, built a new network directly connecting to the PSAPs, and upgraded technology options for every PSAP in Alabama, all on time and within budget as directed by the Alabama State 911 Board.	Leah Missildine State of Alabama Executive Director Alabama 9-1-1 Board Phone: 334-440-7911 Email: leah@al911board.com

The following narrative descriptions highlight the similarities between the projects listed above in the summary matrix and this solicitation, as well as lessons learned throughout those various projects that can be applied to the deployment of the Nebraska ESInet and NGCS solution. Each project narrative includes all subcomponents (items a through e) as outlined above.

Indiana statewide 911 network (IN911)

b. Time Period: 2005 - present
c. Scheduled completion date: NG 9-1-1 as a service, ongoing
Actual completion date: ongoing, with milestones in ‘07, ‘10, ‘12, ‘15, ‘19
d. Bidder’s responsibilities:

INdigital is the prime contractor for the IN911 network. The network was constructed in several stages (or generations). The first System (the G-1 network) was built to establish connectivity from the wireless originating service providers (OSP) using a mated pair of selective routers that were the “front end” for 17 legacy selective routers in Indiana. This network was used to lower costs and improve and monitor the call setup time and accuracy for wireless calls relayed to PSAPs that were connected to the legacy E9-1-1 network.

The second stage of the project (the G-2 network) established direct connectivity from the redundant nodes of the IN911 network to the 120+ PSAPs in the state of Indiana. Direct connectivity with the PSAPs allowed calls to be delivered via a new IP network, eliminating the use of legacy selective routers. These two stages of the project produced significant cost savings for the state (eliminating cost recovery payments to the wireless OSPs), allowed the state to have call statistics, and ensured a uniform level of service throughout the state.

These project stages (which are now even more advanced in our more recent work) are nearly identical to the goals of the Nebraska RFP.

The initial G-1 and G-2 stages of the IN911 network were completed between 2005 and 2008. The network has been upgraded and refined several times since. Beginning in 2011, the network core was refreshed with carrier grade routing hardware. Beginning in 2015, the transport network migrated from a T-1 based network to an ethernet based infrastructure (the G-15 network.) In 2019, the routing core (the G-

19 system) was upgraded to provide improved safeguards for failure scenarios and new types of emergency call delivery options, and to accommodate the direct connection between INdigital's system and the AT&T ESInet. This work is ongoing.

Beyond providing the ESInet, INdigital is the next generation core services (NGCS) provider for the state of Indiana. INdigital has managed the transition of all carriers from the legacy 9-1-1 network to the IN911 network. Initially, INdigital worked with wireless and VoIP carriers throughout the state. In the G-15 and G-19 systems, later wireline OSPs have been added to the network.

INdigital created a service continuity platform, MEVO, which serves as a comprehensive cloud-based backup and disaster recovery system. This platform has endpoints (call taking and mobile units) that are installed in every PSAP. This provides nearly unlimited flexibility in the management and operation of the 9-1-1 system while giving PSAPs new options for dealing with maintenance events and other operational disruptions.

In 2013, INdigital deployed text-to-911 statewide (Texty) over the IN911 network, making Indiana one of the largest statewide deployments of text-FOR-911. INdigital is a text control center (TCC) provider and is also connected to other industry partners serving the wireless OSPs. These connections allow INdigital to seamlessly provide text-to-911 services via its Texty web browser or via an MSRP to enable call handling equipment.

INdigital also manages and operates hosted call handling systems throughout the state of Indiana. INdigital has extensive experience in connecting its NG 9-1-1 system to all types of call handling hosts as is required in this RFP.

e. Contracting Entity:

Indiana Statewide 911 Board
Ed Reuter, Executive Director
ereuter@indigtial.net
317-234-2507

f. The IN911 network was completed by INdigital as the prime contractor. Over the 15-year life of the network, all work has been completed as scheduled and within the proposed budget. Currently, IN911 network is operated at a cost of approximately $11 million annually.

Peninsula Fiber Network - Michigan

a. a. Time Period: 2014 – present

b. Scheduled completion date: multiple
Actual completion date: multiple

c. Bidder's responsibilities:

INdigital has been a subcontractor to Peninsula Fiber Network (PFN) as they have constructed an NG 9-1-1 ESInet throughout the state of Michigan. The project in Michigan began as an effort to build a regional network for the consolidated PSAPs and counties in Michigan's Upper Peninsula Region. INdigital's role has been to provide the NGCS technologies utilized by the ESInet. Initially, INdigital also provided other project management and technical or operational resources to PFN.

After completing the network in the Upper Peninsula Region, additional downstate counties opted to join the network. Beginning in 2014 and continuing through 2020, INdigital has worked with PFN to build a statewide ESInet in the state of Michigan. This project has been unique in the fact that there is not a state agency providing oversight for the network. Rather, the network has been built through the ad hoc effort of PFN, INdigital, and the counties and PSAPs in Michigan.

INdigital has provided all NGCS functional elements for the state of Michigan, including LNG, BCF, ESRP, LPG, ECRF, LVF, NGALI, etc. The state of Michigan enjoys the full complement of software solutions from INdigital, including text-FOR-911, 911 Logix (analytics and MIS), and MEVO.

Additionally, INdigital has been active in managing the conversion of OSPs from the legacy 9-1-1 network to the PFN network. The PFN network is also integrated to several large-scale hosted call handling systems.

d. Contracting Entity:

Peninsula Fiber Network
David McCartney, General Manager
gm@pfnllc.net
906-226-2010

e. INdigital has delivered NGCS services as a subcontractor to PFN for more than five years. Today, the annual budget for these services is in excess of $7 million dollars. Because this was not a state-wide RFP, PSAPs and local jurisdictions have opted into this service. Thus, it is difficult to define project due dates. However, INdigital has worked diligently with PFN for more than five years to ensure the highest level of service to both PFN and the PSAPs of the state of Michigan.

Alabama Next Generation Emergency Network (ANGEN)

a. Time Period: 2016 – present

b. Scheduled completion date: multiple
Actual completion date: multiple

c. Bidder's responsibilities:

INdigital has been the prime contractor for the ANGEN network since 2016. INdigital's role was unique at the outset of this project in that a network had previously been established by another vendor and INdigital was expected to coordinate with the vendor to facilitate the migration to a new network. Our approach was to utilize as many working pieces of the network as possible to maintain the level of service provided to the PSAPs, as well as expedite the transition to the new network. In this case, that meant INdigital would take over the established ingress trunking and coordinate a transition to INdigital's NGCS core, while establishing connectivity to the legacy network to provide call delivery to the PSAPs.

In our role as the prime contractor, INdigital is responsible for providing ingress OSP aggregation and migration to all wireless, wireline and VoIP carriers in Alabama; Next Gen Core Services, including, BCF, SBC, ESRP, LDB, ECRF, LVF, text-for-911, MEVO, 911 Logix (visualization and analytics); and, ESInet connectivity to each PSAP and call handling host in the state.

The core functional elements of the network were deployed in 2017 and a multi-stage transition of PSAPs to the network began the following year. The staged approach includes three separate phases:

1. Establish ESInet connectivity to PSAPs and call handling hosts and establish gateways to pick up locally delivered 911 traffic.
2. Deploy "new" services to PSAPs, including the MEVO service continuity platform, text-FOR-911 and 911 Logix.
3. Migrate locally delivered 9-1-1 traffic to direct connections to the NGCS core.

This staged approach to transition allows the new network to quickly begin providing valuable services to PSAPs, while setting the stage for a successful migration of traffic for the legacy network to the ANGEN network.

d. Contracting Entity:

Alabama 911 Board
Leah Missildine, Executive Director
leah@al911board.com
334.440.7911

e. A prime contract valued at approximately $52M was signed between INdigital and the Alabama 911 Board in 2016. Since then, INdigital has taken over the existing network, built a new network directly connecting to the PSAPs, and upgraded technology options for every PSAP in Alabama, all on time and within budget as directed by the Alabama 911 Board.

vi. Contractor and subcontractor(s) experience should be listed separately. Narrative descriptions submitted for subcontractors should be specifically identified as subcontractor projects.

Hamilton has submitted three (3) NG 9-1-1 narrative project descriptions as specified above in Summary of Bidder's Corporate Experience (item h). Within these project descriptions, Hamilton has differentiated work completed as a subcontractor (for example, the Peninsula Fiber Network – Michigan) and outlined contract costs, project responsibilities and the time period serving as a subcontractor.

vii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the Contractors above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

Hamilton has submitted three (3) NG 9-1-1 narrative project descriptions as specified above in Summary of Bidder's Corporate Experience (item h). Within these project descriptions, Hamilton has differentiated work completed as a subcontractor (for example, the Peninsula Fiber Network – Michigan) and outlined contract costs, project responsibilities and the time period serving as a subcontractor.

i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this solicitation. The names and titles of the team proposed for assignment to the State project should be identified in full, with a description of the team leadership, interface and support functions, and reporting relationships. The primary work assigned to each person should also be identified. Project managers assigned to the project shall be certified Project Management Professionals (PMP) and are highly encouraged to possess the Emergency Number Professional (ENP) certification.

The bidder should provide resumes for all personnel proposed to work on the project. The State will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the solicitation in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the State.

Hamilton and its subcontractors, INdigital, GeoComm, DDTI, and NebraskaLink (detailed below), have a significant group of qualified, experienced professionals who will be assigned to this project to fulfill the requirements of the RFP. Our team has superior depth and reach when it comes to designing, implementing, and supporting projects similar in size and scope as the Nebraska NG 9-1-1 project. As such, we utilize staff with the appropriate skill sets to efficiently staff projects like these to ensure successful and timely delivery and contract performance.

The following organizational chart for Hamilton has been included to show lines of authority of personnel involved in the performance of this contract.

Organizational Chart

Hamilton has a significant number of key executive and professional personnel engaged to work on this project and is committed to allocating quality personnel to fulfill all objectives of the implementation. The following chart provides an overview of these individuals and their qualifications. In addition, resumes and references for all listed personnel are provided within Appendix 5 – Hamilton Resumes and References.

HAMILTON KEY PERSONNEL

(Listed in Alphabetical Order)

TEAM MEMBER	TITLE	QUALIFICATIONS
Peggy Christensen	Project Manager, PMP	• Certified PMP. • 15+ years of project management experience. • 15+ years' experience in leading teams, management and performance / enterprise project curation.
Jim Ediger, J.D.	Senior Regulatory Compliance Expert, Hamilton NG911	• 8+ years of legal, contract and regulatory representation experience. • In-house counsel for seven diverse business entities. • Legal liaison for Senior Management and company representative on public safety working groups.
Wayne Hahn	WAN Manager and Network Engineer, Hamilton NG911	• 30+ years of IT experience specializing in Wide Area Network management. • Ensures network systems operate sufficiently. • Develops standards and procedures to ensure quality assurance; reviews change control processes and regulatory adherence.

Jeffrey Knighton	President, Hamilton Innovations	• 20+ years' experience in designing, developing, and deploying telecommunication and accessibility products. • Managing new products and software development. • Research and technical assistant for NG 9-1-1 and Traditional Relay Service Technology.
Robert Leonard	Security Manager, Hamilton NG911	• 20+ years of IT, Cyber Security, LAN Admin, Network management and Backup/Recovery Implementation Management experience. • CompTIA Security + Certified • Security audits and program management of active directory networks.
Seth Marks	Vice President of Engineering, Hamilton Innovations	• 16+ years' experience in product development. • Team lead for integrated programs, project design and deployment. • New software development.
Dan Molliconi	Chief Operating Officer	• Member of Senior Management • 25 years experience in human resource management and corporate telecommunications and technology leadership.

John Nelson	President & Chief Operating Officer Hamilton NG911	• Lead Member of Senior Management • 25 years of leadership experience in the telecommunications and Relay Industries
Gary Warren	Senior Consultant, Hamilton NG911	• 30+ years' experience in leadership of diversified telecommunications, business development, government regulation, legal expertise and senior leadership.
Ryan Wineteer	Manager, Hamilton NG911	• 10+ years' experience in technical sales and technical project management.
Dixie Ziegler	President of Nedelco Services Corporation & Chief Operating Officer, Hamilton Relay Services	• Member of Senior Management • 25 years of corporate leadership and national division operations experience. • Dynamic leader of teams and innovative accessibility advocacy and solutions. • National branding and identity for Hamilton Relay Services

In addition to the personnel listed above (almost all of whom work and live in Nebraska), Hamilton has over 1,000 employees nationwide at its disposal that can assist, if needed, in various capacities. Overall, Nebraska will find that the Hamilton team has the required experience and qualifications, including education and training, to meet the project's requirements.

Further, in addition to Hamilton's staffing resources, Hamilton's subcontractors will provide a significant number of qualified, experienced professionals who will be assigned to this project to fulfill the requirements of the RFP. As described in detail below within our Subcontractors' response, Hamilton has contracted with INdigital to provide their technology and expertise. INdigital will be the primary subcontractor and NGCS technology provider and will provide NOC/SOC services to the state as a subcontractor to Hamilton. Hamilton NG911 will be the prime contractor to the state of Nebraska, fulfilling the primary project management role, ESInet implementation and will be ultimately responsible for the success of this project. Hamilton has also contracted with GeoComm, DDTI, and NebraskaLink. Cumulatively, GeoComm and DDTI will provide all GIS functional elements. More specifically, GeoComm is providing the SI/ECRF/LVF and DDTI is providing the location services

to replace legacy ALI systems in the form of both an MCS (MSAG Conversion Service, to support PSAPs that still require legacy ALI) and LDB (Location Database, full legacy ALI replacement). Lastly, Hamilton will leverage its relationships with NebraskaLink and their national network relationships to provide the IP network infrastructure as well as the ingress traffic interconnection from the OSPs.

Staffing charts for INdigital, GeoComm, DDTI, and NebraskaLink provide an overview of these individuals and their qualifications. These staff members are experienced in similar installations and training is current.

The following chart details designated staff on behalf of INdigital who will be working alongside Hamilton on the Nebraska NG 9-1-1 project. Hamilton's Project Manager, Peggy Christensen, PMP, will be responsible for overseeing the work of INdigital and ensuring collaboration occurs throughout the course of the project by all entities involved.

INDITIGAL KEY PERSONNEL
(listed in alphabetical order)

TEAM MEMBER	TITLE	QUALIFICATIONS
Kent Claussen	Chief Technology Officer	• 30+ years' experience in IT and Telecom. • Network and programming focus. • Fluent in most modern programming languages and methodologies.
Mark Grady	Founder and President	• 35+ years' experience as an innovative leader in Telcom. • Technical, operational, planning and management expertise. • Network system design and technology innovation.
Eric Hartman	Executive Vice President	• Nearly two decades of IT experience. • 9-1-1 product management. • Support and managing projects.

An explanation of GeoComm's proposed approach to the management of the project, including the ECRF, LVF, and GIS Data Hub scope of work is detailed on the following pages, followed by their list of professionals designated for the Nebraska NG 9-1-1 project.

GeoComm ECRF and LVF Scope of Work

GeoComm's ECRF and LVF will be deployed in Hamilton's data center. Hamilton will be responsible for managing the systems, including monitoring, alarming, hardware support and backups. GeoComm will also monitor the system and be responsible for Tier II support services.

Project Approach

The project will be executed in the following phases:

- Phase One: Project Initiation
- Phase Two: ECRF, LVF, and MCS Implementation
- Phase Three: ECRF and LVF Software Training
- Phase Four: Software Acceptance Testing
- Phase Five: Post-Deployment Support Services

PHASE ONE: PROJECT INITIATION

The ECRF and LVF project will be initiated with a remote project initiation meeting. The meeting will be held with the State and Hamilton representatives, as well as GeoComm's Project Manager. In the Project Initiation meeting, Hamilton will:

- Introduce key personnel
- Review project objectives and goals
- Define mutual expectations
- Establish communication processes
- Discuss the project schedule, including frequency of periodic progress reporting

PHASE TWO: ECRF AND LVF IMPLEMENTATION

Hamilton staff and a GeoComm Implementation professional will work collaboratively to complete the following pre-implementation tasks:

- Remote system staging
- Remote testing of base system installations and modules
- Remotely assist in complete system redundancy testing
- Configuration of system testing tools
- Configuration for provisioning services

After these tasks are complete, the GeoComm ECRF, LVF, and MCS will be deployed in Hamilton's data centers. All implementation and configuration tasks will be completed remotely.

PHASE THREE: ECRF AND LVF SOFTWARE TRAINING

ECRF and LVF training will be provided remotely. It will focus on the functions and architecture of the software. In addition, training will provide an overview of the ECRF and LVF systems within the overall NG 9-1-1 system. The provisioning process and maintenance of the system will also be covered. Key data quality processes will be included in the course along with descriptions of interfaces. The State will be responsible for determining the appropriate staff to participate in the training sessions. Typically, IT or administrative professionals and a lead GIS technical representative attend the training. To ensure the State can perform Tier I support services, if desired, on the ECRF and LVF system, Hamilton and GeoComm will train appropriate staff on system triage and troubleshooting procedures. During the training session, Hamilton and GeoComm will work collaboratively to establish a support standard operating procedure and document required protocols for resolutions and triage of issues prior to escalating for Tier II support.

PHASE FOUR: SOFTWARE ACCEPTANCE TESTING

After implementation and training are complete, testing measures will be coordinated to ensure interoperability between applications. In addition, GeoComm and Hamilton will test integration points to ensure seamless incorporation of the ECRF, LVF, and MCS into the State's NG 9-1-1 system. The testing measures will be executed prior to system go-live.

A software acceptance test plan will be completed to ensure product performance has been tested. The GeoComm technical team comprised of Implementation Specialists, Software Development, Testing, and Support Analysts will work with Hamilton's technical team to ensure all functionality contracted for is included in the final system. If any gaps are identified, a plan for resolution will be developed.

PHASE FIVE: POST-DEPLOYMENT SUPPORT SERVICES

Hamilton and GeoComm will work closely to ensure services are delivered as contracted for and to the State's satisfaction. Tier II support services for the ECRF and LVF will be provided. Hamilton will provide Tier I support, escalating issues to the GeoComm support team for resolution. Overall, support services will be provided by Hamilton and GeoComm and will include software support technicians, GIS specialists, and project management professionals.

To ensure the State understands the support service protocol for system troubleshooting, Hamilton and GeoComm will train State staff on the processes and procedures required to provide effective first-line support. In the event a technical issue cannot be resolved, and after following pre-established Tier I protocols, the issue will be escalated to Tier II software support services.

GeoComm GIS Data Hub and SI Scope of Work

Hamilton's proposed solution includes GeoComm's NG 9-1-1 GIS implementation services paired with GeoComm GIS Data Hub and spatial interface (SI) to fully meet Nebraska's NG 9-1-1 GIS data management goals. GIS Data Hub is a user-friendly, fully integrated NG 9-1-1 GIS data management application which provides a means to ingest, analyze, report, and merge GIS data. GIS Data Hub was developed to accomplish the following ongoing GIS data tasks:

- Submission of data to a centralized authority
- Quality Control (QC) processing
- Transformation to a common GIS data schema
- QC validation for NG 9-1-1 call routing and NENA standards
- Merging multiple datasets into one seamless statewide dataset
- Quality reporting
- Provisioning to NG 9-1-1 core components (the NENA Spatial Interface)

NG 9-1-1 GIS Implementation Services

The primary goal of the NG 9-1-1 GIS Implementation Services will be to develop a repeatable workflow for processing GIS data, resulting in a continuous feedback loop on the quality of the GIS data updates from local jurisdictions. Project stakeholders will interact with GIS Data Hub in the following way:

- The State or local jurisdictions (depending on the final contract) will upload GIS data to GIS Data Hub, following a mutually agreed upon up-to-daily frequency schedule
- Data will undergo QC checks adhering to NENA and State-required standards
    - The State may choose to set processing thresholds customized to each layer that, if triggered, would prevent data from being incorporated into the merged dataset
    - The submitting agency will be notified and will receive a report explaining the reason for the failure
- Data quality reports will be delivered to submitting agencies via GIS Data Hub
- The State or local jurisdictions will correct errors outlined in the QC reports and resubmit updated data back to GIS Data Hub
- After the data is evaluated with the QC checks, it is transformed into the format required for NG 9-1-1 and merged into the statewide dataset
- A final statewide GIS dataset will be provisioned to the GeoComm ECRF and LVF

Project Approach

Hamilton and GeoComm will collaboratively work with the State to execute a series of specific GIS and technical tasks to successfully deploy GIS Data Hub at the State, including tasks to achieve a GIS dataset that meets requirements for geospatial call routing.

This will include collaboration with the State or local jurisdictions to ensure data sources are identified and analyzed for readiness in GIS Data Hub and, if data aggregation/merging services are required, are merged into a Statewide dataset for ECRF and LVF operations. This will include identifying edge-matching resolutions recommended to create a seamless dataset for call routing.

The project will be completed in the following phases:

- Phase One: Project Initiation
- Phase Two: GIS Data Management Workflow Collaboration
- Phase Three: GIS Data Hub Configuration and Data Load
- Phase Four: Interoperability Testing
- Phase Five: Field Mapping Review and Coordination
- Phase Six: GIS Data Hub System and Process Training
- Phase Seven: Merged Geodatabase Creation (if required)
- Phase Eight: GIS Derived MSAG Development and Processing
- Phase Nine: Ongoing Operational Support

It is anticipated the phases will occur in a mostly chronological order as listed, though some will take place simultaneously. Throughout each phase, time is dedicated to project management and ongoing communication with the State to ensure that deliverables are being met and project objectives are being carried out. Hamilton and GeoComm will work together to provide regular status updates that will include:

- General progress updates
- Meetings held, planned, or needed
- Issues/problems encountered or anticipated
- Goals for the next reporting period
- Schedule review
- State and local jurisdiction responsibilities

A detailed description of each phase is provided below.

PHASE ONE: PROJECT INITIATION

Project Initiation Meeting

Hamilton will coordinate a Project Initiation meeting to be scheduled and conducted with the State's project team, the GeoComm Project Manager, and a GeoComm GIS Specialist. The meeting agenda will include:

- Introductions and identification of project team members and roles
- Timeline and deliverable review
- Project approach review
- Project communication methods

PHASE TWO: GIS DATA MANAGEMENT WORKFLOW COLLABORATION

GIS Data Management Workflow Collaboration Meeting

Following the Project Initiation meeting, Hamilton and GeoComm will conduct a remote GIS Data Management Workflow Collaboration meeting to document a GIS Data Hub GIS data workflow and QC plan. Policies for regular, ongoing GIS data submittal to GIS Data Hub will be established. A QC plan, including regular communication of QC results to counties, will be documented. The QC plan will detail quality control processes to be performed on GIS data submitted to GIS Data Hub. The meeting will cover the following topics:

- GIS data submission and reporting interface demonstration
- Standard workflow procedures
- Review of the State's data schema and critical errors for ECRF and LVF
- Data schema field mapping processes
- Attribute standards
- QC error options review
- Initial workflow diagram development
- Seamless dataset development and maintenance process

In addition, if aggregation services are contracted for, Hamilton and GeoComm will work with project stakeholders to initiate data collection from the counties (GIS, MSAG, and ALI). This will include assisting counties with obtaining the required project data. However, the counties will be responsible for all third-party fees which may be required to obtain copies of the required project data (i.e. MSAG and ALI).
After the conclusion of the Project Initiation meeting, collaboration with the State will occur to execute a series of tasks to draft, refine, and deliver GIS data workflows which incorporate steps needed for continual operation of GIS processing.

GIS Data Management Workflow Development

Following the GIS Data Management Workflow Collaboration meeting, preliminary NG 9-1-1 management workflows will be developed which incorporate utilizing GIS Data Hub for NG 9-1-1 GIS data tasks. Documentation, including diagrams depicting the workflows, will be provided to the State for review. The NG 9-1-1 GIS workflows would cover roles, responsibilities, and activities including:

- Local QC error report and remediation management workflow
- Process overview, including merging GIS updates into the Statewide GIS dataset if aggregation services are contracted for
- ECRF and LVF provisioning and error notification workflow

After project stakeholders have time to review the preliminary workflow documentation, up to two additional conference calls will be conducted and/or working web sessions to discuss and adjust the workflow diagrams.

PHASE THREE: GIS DATA HUB CONFIRURATOIN AND DATA LOAD

After the GIS Data Management Collaboration meeting, Hamilton and GeoComm will work together to begin configuring GIS Data Hub for the State. Industry standards, the State's required system deployment and system usage, and GeoComm's experience will be accounted for when configuring the final system.

Initial Data Load and Data Configuration

Before the State and, if optional aggregation services are contracted for, local jurisdictions can leverage GIS Data Hub for data QC and reporting functions, optionally, data aggregation, source GIS data must be loaded and configured in the system. This will be accomplished by working with the State to import data into the system. Accounts for users authorized to upload data will be created and users will then upload their initial datasets. As part of this process, field mapping and QC check configuration tasks will be completed.

GIS Data QC Checks Processing

After local source datasets have been uploaded and configured in GIS Data Hub, the datasets will undergo QC checks processing. The QC checks will be executed and will report concerns with topology and data integrity. They will also include evaluation of spatial and attribute data based on compliance with NENA and State data model standards.
The State will receive a report with QC check findings. The State will be responsible for updating the data to adhere to applicable standards. If aggregation services are contracted for, each local source data authority will receive a report with QC check findings. Local data authorities will update the data to adhere to applicable standards.

PHASE FOUR: INTEROPERABILITY TESTING

Hamilton and GeoComm will coordinate testing measures to ensure interoperability between GeoComm SI and the ECRF. This will include working with project stakeholders to ensure all system functionalities contracted for have been delivered. If any functionality gaps are identified, a plan for resolution will be developed.

PHASE FIVE: FIELD MAPPING REVIEW AND COORDINATION

To control how GIS data is processed and ultimately written to the final data output, GIS data must be configured into GIS Data Hub. The one-time field mapping process will allow the State (or local jurisdictions, if aggregation services are contracted for) to continue working in your existing data structure as long as all mandatory and conditional fields are represented in the source dataset. Entities will each submit information about their data which will then be used to conduct field mapping.

PHASE SIX: GIS DATA HUB SYSTEM AND PROCESS TRAINING

Hamilton and GeoComm will collaboratively hold a meeting to distribute and discuss the GIS Data Management workflows finalized following the GIS Data Management Workflow Collaboration meeting. The workflows will outline the flow of GIS data through the system. In addition, GIS Data Hub training services will be provided at this time. Training will provide the subject matter and materials required for system users to successfully leverage the system, including the GIS data management workflows, including:

- Access to GIS Data Hub
- GIS Data upload
- QC settings and field mapping
- QC results notification receipt and download

- Accessing the QC summary report
- Workflow diagram and User Guide review
- Review of QC process results
- Correcting reported errors
- Q&A

Training Audiences

It will ultimately be up to the State to determine who will attend the courses. Generally, user roles will be defined by responsibilities around GIS data QC and maintenance. Hamilton and GeoComm will work with the State to define these roles and establish the best participants for whichever training courses are selected.

PHASE SEVEN: MERGED GEODATABASE CREATION (IF REQUIRED)

If the State does not submit one single statewide GIS dataset to the system (if data aggregation services are required), after local GIS data is submitted to GIS Data Hub and passes the QC checks within GIS Data Hub, it will be merged into a statewide GIS dataset to support NG 9-1-1 call routing.

Automated schema and geodetic transformation procedures will be executed to assimilate the source GIS data layers into an authoritative GIS data model compliant with the State's and NENA's evolving NG 9-1-1 data standards. The GIS dataset will incorporate existing data from the local jurisdictions. The individual GIS data layers will then be merged into a statewide dataset.

After the data has been merged into a statewide dataset, it will again be processed through configured QC checks to determine the quality of the merged dataset. Results will be reported back to the State. Counties will be responsible for resolving errors found within their respective datasets and work with neighboring jurisdictions to resolve topology errors.

PHASE EIGHT: GIS DERIVED MSAG DEVELOPMENT AND PROCESSING

The proposed solution includes one-time services to build a GIS derived Master Street Address Guide (MSAG), as well as MSAG delta processing services to assist the State with maintaining ongoing synchronization between the State's NG 9-1-1 Road Centerline layer, and the aforementioned GIS derived MSAG used by the Location Database (LDB).

GIS Derived MSAG Development

This task is accomplished by utilizing the statewide Road Centerline layer and building a tabular MSAG based of the attributes included (referenced above as GIS derived MSAG). This service includes QC and verification that the deliverable meets the needs of the LDB provider, DDTI.

MSAG Delta Provisioning

Once the GIS derived MSAG has been built, the ongoing process of detecting and delivering MSAG deltas will begin. This process consists of:

- Gathering the most current GIS data from GeoComm GIS Data Hub for the State's project
- Generating MSAG deltas via the changes detected to the State level GIS data on a once daily basis
- Modifying the delta file to conform to NENA 2.x format
- Performing QC checks to ensure the GIS changes create logical MSAG modifications
- Passing the files to the LDB provider by copying to an agreed upon location, such as using email, SFTP, or a web portal location

Hamilton and GeoComm will work cooperatively with the state and LDB provider, DDTI, to establish a regular schedule for these services.

PHASE NINE: ONGOING OPERATIONAL SUPPORT

Ongoing GIS Data Transformation, QC, and Reporting

GIS Data Hub will provide ongoing GIS data transformation, QC, and reporting which will result in the progressive improvement of the Statewide NG 9-1-1 GIS dataset. In addition, should aggregation services be required to merge disparate local GIS dataset into one statewide GIS dataset, ongoing data merging services would be executed by GIS Data Hub, resulting in the progressive improvement of a single, seamless Statewide NG 9-1-1 GIS dataset. Note that managed services by Hamilton and GeoComm would begin for each local jurisdiction after the initial load into GIS Data Hub is complete.

The ongoing services workflow will follow a similar workflow to that of the initial data upload, QC, and merging. As follows:

- The State will upload a single, statewide GIS dataset updates to GIS Data Hub on an up-to-daily basis.
    - If data aggregation services are required, individual Counties would upload GIS data updates to GIS Data Hub on an up-to-daily basis.
- GIS data will undergo multiple configured QC checks.
    - The QC checks will report concerns with topology and data integrity, and ultimately ensure only accurate GIS data is included in the NG 9-1-1 GIS dataset used in ECRF and LVF.
    - The QC checks will include evaluation of spatial and attribute data based on compliance with NENA and State data model standards.
- Data quality reports will be delivered to the State (or each respective local jurisdiction if aggregation services are contracted for). The State/Local jurisdictions will be responsible for updating data to adhere to the applicable standards.
- Source jurisdictions will correct the GIS data errors outlined in the data quality reports provided by the system and resubmit updated data back to GIS Data Hub.
    - Source jurisdictions may find the data quality reports to be beneficial in determining the roles, responsibilities, authority, experience, training, and ongoing hours of effort it will require to improve the data for NG 9-1-1.
- After the data is evaluated with the QC checks, it is transformed into the format required for the NG 9-1-1 System
    - If data aggregation services are contracted for, the data is merged into a statewide NG 9-1-1 GIS dataset and an additional round of QC checks is performed to ensure there were no issues created during the data merging process which would cause errors.
- After data has passed QC checks, it is transferred from the GeoComm SI to the ECRF and LVF for geospatial call routing.

This process will result in a continuous feedback loop of GIS data updates from the local jurisdictions, GIS data performance measurements and reporting, data transformation, and merged.

Synchronization with the MSAG and ALI Database

As part of every map data upload, GIS Data Hub will perform a comparison between the GIS data and the MSAG, and the GIS data and the ALI Database and report results back to local authorities. The results will be a valuable resource for local authorities in keeping their GIS data synchronized with the MSAG and ALI database, as well as a metric for measuring progress toward required synchronization levels. Results will be compiled into reports and made accessible to the State and counties. A new ALI and MSAG are not required for each upload. Comparisons will be completed on the most recent data, ALI, and MSAG submitted. It is important to note that if end users update their MSAG and ALI databases as a result of reported discrepancies, the same discrepancies will continue to be reported until an updated MSAG and ALI are submitted for fresh comparison.

Merged NG 9-1-1 GIS Database Provisioning

After the data has been merged and has passed required QC checks, it is transferred from GeoComm SI to the ECRF and LVF for geospatial call routing. The GeoComm SI is a NENA i3 compliant Spatial Interface (SI) for transmitting GIS data updates from the authoritative GIS database system and applying to ECRF and LVF database. In addition, the GeoComm SI supports non-NENA-standard ECRF and LVF GIS database update formats such as Esri file geodatabase.

In order to accomplish the scope of work outlined above for the ECRF/LVF and GIS Data Hub, Hamilton and GeoComm have assembled a project team with experienced, skilled industry professionals who are at the forefront of deploying NG 9-1-1 GIS across the nation. Specifically, the GeoComm project team will be led by GIS project managers Sean Lehman GISP, ENP, who will oversee GeoComm's project elements and serve as a liaison between GeoComm, Hamilton, and the State. The remainder of GeoComm's project team is comprised of a combination of professionals from the Client Services division, including GIS managers, technicians and trainers, implementation managers, technicians, and trainers. Client Services' efforts will be overseen by Implementation Manager Jodi Wroblewski, PMP, and GIS Manager Hanna Lord. This team has

worked together on dozens of NG 9-1-1 GIS projects to successfully help our customers transition to GIS-based call routing for 9-1-1.

As mentioned throughout this section specific to GeoComm's proposed approach to the management of the project, including the ECRF, LVF, and GIS Data Hub scope of work, significant collaboration will occur over the course of the project between Hamilton and GeoComm. Hamilton's designated Project Manager, Peggy Christensen, PMP, will be overseeing the work completed by GeoComm.

GEOCOMM KEY PERSONNEL
(in alphabetical order)

TEAM MEMBER	TITLE	QUALIFICATIONS
Sean Lehman	GIS Project Manager, GISP, ENP	• 20+ years' experience in GIS specialization and management. • Expertise in client communication, project-level satisfaction, meeting project needs and implementing updated software.
Jodi Wroblewski	Implementation Manager	• 16+ years' experience in project management and leadership in public safety. • Manages resources focused in implementation of software products, installation and training services.
Hanna Lord	GIS Manager	• 8+ years' experience in GIS implementation and management in public safety. • Oversees the development of quality GIS data, training, and monitoring.

As mentioned earlier, Hamilton has contracted with DDTI to provide the location services necessary to replace legacy ALi systems in the form of both an MCS (MSAG Conversion Service, to support PSAPs that still require legacy ALi) and LDB (Location Database, full legacy ALi replacement). DDTI has designated a project team to coordinate and provide these GIS functional elements. Additionally, in order to successfully integrate these GIS functional elements into the Hamilton solution, Hamilton will provide Peggy Christensen, PMP, to oversee the work of DDTI and to assist with collaboration between all entities involved in providing Nebraska's NG 9-1-1 solution. DDTI staff is listed below:

DDTI KEY PERSONNEL
(in alphabetical order)

TEAM MEMBER	TITLE	QUALIFICATIONS
John Browning	System Implementation Coordinator, PMP	• 15 years' experience in GIS for 9-1-1. • Focus on software upgrades, testing and staging environments and implementation.
Tony Collura	Director of Operations	• 20 years of experience in project management, GIS/GPS analysis and leading teams. • Has contributed to 50+ GIS data normalization projects.
Tessa Haizel-Cobbina	Location Database Services Coordinator	• 13+ years' experience in electronic engineering and 9-1-1 industry. • Specializing in ALI database systems, LDB updates and workflows.
Craig Hamm	Systems Engineer	• Over 20 years' experience in network engineering and 9-1-1 systems. • MCSE, MCSA and Windows Server certifications.
Mitch Pinkston	Chief Information Officer	• 17+ years' experience in project management, GIS/GPS analysis, and leadership. • Oversee NG 9-1-1 requirements, standards, and operational practices.

Lastly, Hamilton is contracting with NebraskaLink for the use of their statewide fiber optic network that provides broadband transport and ethernet access across the state of Nebraska and beyond. As one of the five owners and founding partners, Hamilton is extremely familiar with working with NebraskaLink and has done so for a significant period of time in order to provide unparalleled service across the state of Nebraska to entities in many sectors where high reliability and dependability are key. NebraskaLink is also providing a team of professional staff dedicated to ensuring the success of the Nebraska NG 9-1-1 project and, as mentioned earlier in previous sections highlighting subcontractor staff, Peggy Christensen, PMP, will be responsible on behalf of Hamilton to oversee and coordinate the work between Hamilton and NebraskaLink. NebraskaLink staff is highlighted in the chart below:

NEBRASKALINK KEY PERSONNEL
(in alphabetical order)

TEAM MEMBER	TITLE	QUALIFICATIONS
Chris Johnson	Director of Operations	• 20+ years' experience in field and network operations, project management and leadership. • Extensive knowledge of OSP, ISP, engineering, transport, pricing, OAM, process creation, business continuity and development and operational software.
Brent Timothy Lamb	Operations Manager	• 23+ years' experience in telecommunications, team development and exceed business objectives. • Expertise in project management, network design, operations management, engineering and administration.
Marissa Munch	Service Assurance and Project Manager, PMP, PMI-ACP	• 10+ years' experience in project management, leading teams and cross-cultural professional communications. • Certified project manager overseeing implementation, milestones and overall coordination.

Mark Shaw	Chief Executive Officer	• 22+ years' experience in project management and senior leadership. • Expertise in project management, pricing and provisioning models, business development and leading dynamic teams.
Don Uhrmacher	Service Support Manager	• 40+ years' experience in telecommunications performance, development and leadership. • Extensive experience in all facets of network testing and support, budgeting, reports creation, customer support, vendor management, and database and hardware administration.

In conclusion, resumes and references for all subcontractor staff are included in Appendix 5 – Hamilton Resumes and References. All resumes include academic background and degrees, professional certifications, and professional references. While telephone numbers and addresses of references are not provided within this response, Hamilton is prepared and willing to provide all additional information as needed. Hamilton understands that any proposed changes in personnel should only be implemented after first obtaining written approval from the State.

j. SUBCONTRACTORS
If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

i. name, address, and telephone number of the subcontractor(s);

Hamilton will be utilizing the following subcontractors in the fulfillment and completion of the awarded contract: Communications Venture Corporation ("INdigital"), Geo-Comm ("GeoComm"), Digital Data Technologies Inc. ("DDTI") and NebraskaLink Holdings, LLC. ("NebraskaLink").

INdigital is an Indiana Corporation with a principal place of business at 1616 Directors Row, Fort Wayne, Indiana, 46808. Their main point of contact is Mark Grady, Founder and President. His contact information is as follows: 260-469-2010 (office) and mgrady@indigital.net.

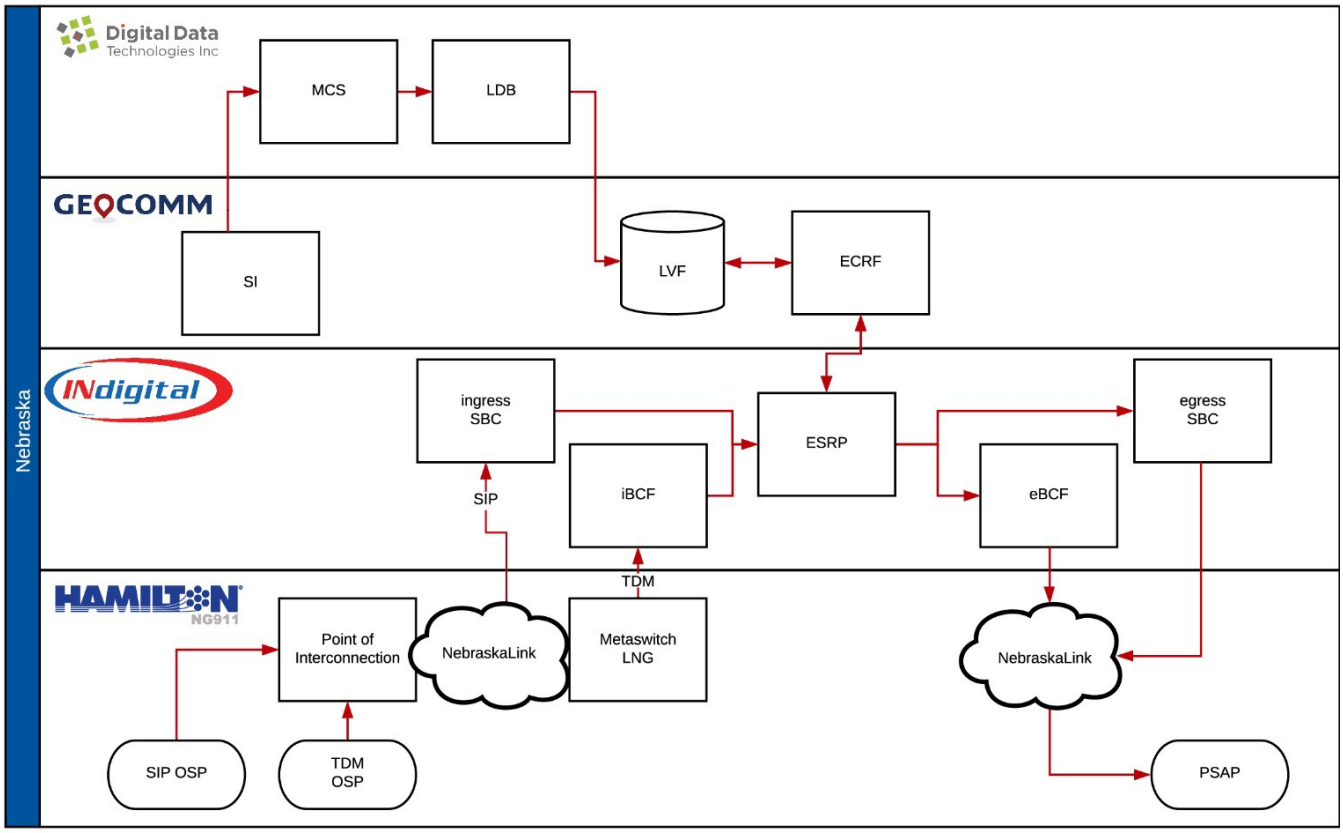
GeoComm is a Minnesota Corporation with a principal place of business at 601 West St. Germain Street, Saint Cloud, MN, 56301. Their main point of contact is Stacen Gross, ENP, Territory Sales Manager. His contact information is as follows: 402-321-0817 (cell) and sgross@geo-comm.com.

DDTI is an Ohio Corporation with a principal place of business at 2323 W. Fifth Avenue, Suite 210, Columbus, OH, 43404. Their main point of contact is Chris Santer, Vice President and Owner. His contact information is as follows: 614-429-3384 (office) and csanter@ddti.net.

NebraskaLink is a Nebraska Corporation with a principal place of business at 3900 NW 12th St., Suite 100, Lincoln, NE 68521. Their main points of contact include Marissa Munch, Service Assurance/Project Manager, and Brent Lamb, Operations Manager. Ms. Munch's contact information is as follows: 402-621-2374 (cell) and marissa.munch@nebraskalink.com. Mr. Lamb's contact information is as follows: 402-817-1842 (cell) and brent.lamb@nebraskalink.com.

ii. specific tasks for each subcontractor(s);

The following diagram clearly depicts the subdivisions of project description and scope of work for Hamilton and its subcontractors:



Hamilton has determined that INdigital, GeoComm, DDTI, and NebraskaLink are the best vendors to fulfill the requirements of Nebraska's NG 9-1-1 contract. Hamilton will remain solely responsible for the performance of its obligations under the resulting contract and feels strongly that utilization of these subcontractors will allow Hamilton to deliver the highest quality solution while sustaining its implementation schedule and budget. Hamilton NG911 is bringing the best of the best in each core NG 9-1-1 segment to the state of Nebraska.

Further, INdigital and GeoComm are leading providers of NG 9-1-1 services, specializing in NENA i3 compliant solutions. As described in significant detail throughout this Corporate Overview section, Hamilton has contracted with INdigital to provide their technology and expertise to help ensure a successful outcome. INdigital will be the primary subcontractor and NGCS technology provider and NOC/SOC services to the state as a subcontractor to Hamilton. As outlined in the diagram above, Hamilton has also contracted with GeoComm, DDTI, and NebraskaLink. Together, GeoComm and DDTI will provide all GIS functional elements. GeoComm is providing the SI/ECRF/LVF, and DDTI is providing the location services to replace legacy ALI systems in the form of both an MCS (MSAG Conversion Service, to support PSAPs that still require legacy ALI) and LDB (Location Database, full legacy ALI replacement). Lastly, Hamilton will utilize its relationships with NebraskaLink and their national network relationships to provide the IP network infrastructure as well as the ingress traffic interconnection from the OSPs.

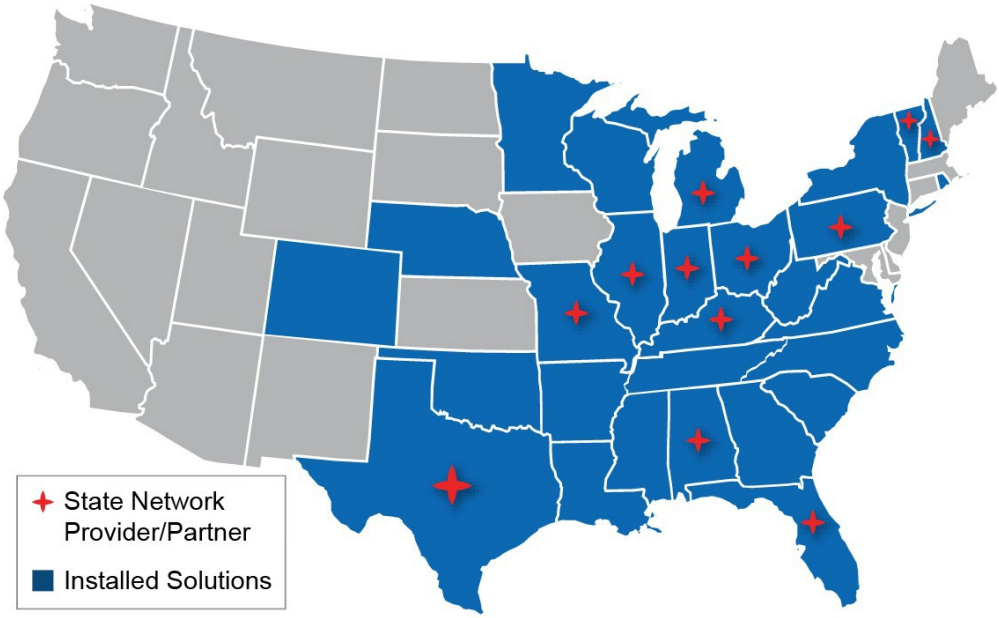
The following information provides more details on Hamilton's subcontractors and further substantiates why Hamilton and its subcontractors are qualified to fulfill all requirements of Nebraska's NG 9-1-1 project:

INdigital is a next generation public safety research and development company based in Fort Wayne, Indiana. The company is owned by nine independent telephone companies in Indiana, Michigan, and Ohio. It began providing IP-based 9-1-1 service in 2005 for the state of Indiana, prior to the development of NENA i3 standards.

Since then, the company has grown and advanced, providing service either directly, or through similar teaming agreements in 11 states, serving 500+ public safety answering points (PSAPs), and serving a population of 40 million.

The company has processed and delivered more than 35 million IP-based 9-1-1 calls to over 1,000 distinct IP-based endpoints, utilizing several different NG 9-1-1 compliant methods to many types of systems. The company has a number of projects now underway, including an integration with the AT&T Indiana MicroData platform and an established tri-state ESInet with the Cincinnati Bell MicroData platform, both maintained by Comtech.

INdigital is widely recognized as an industry thought leader and ESInet design/ build/operate 9-1-1 service provider. Additionally, INdigital has successfully created, delivered, and operated many first to market and best in class NG services.



The above map reflects INdigital installed solutions.

Together, Hamilton and INdigital have developed several advances in the NG core service industry segment and share the common goal of advancing the industry.

GeoComm was founded on May 18, 1995, to provide local governments with turnkey emergency 9-1-1 software and GIS services. Over the subsequent 24 years, the company has grown to serve emergency professionals in over 1,000 public safety answering points (PSAPs) throughout the United States, helping to keep more than 100 million people safe. Today, GeoComm has a national reputation as a leading provider of public safety GIS software solutions and services.

Since its founding, GeoComm has assisted its customers to implement public safety grade GIS solutions that includes data development, maintenance services, mapping and dispatch applications, and NG 9-1-1 core component such as emergency call routing function (ECRF), location validation function (LVF), spatial interface (SI) and data validation solutions to offer the best possible emergency services. GeoComm's professional staff has diverse, comprehensive industry experience from their public safety involvement dating back to the advent of basic 9-1-1. This experience has grown substantially as the company has assisted hundreds of jurisdictions across the nation to deploy Enhanced 9-1-1 (E9-1-1) software and services. It continues to evolve today through innovation, customer engagements and active participation in industry groups who are helping to shape the future of NG 9-1-1.

Over the last several years, GeoComm has become a proven provider of end-to-end GIS systems tailored to meet the needs of public safety agencies moving to NG 9-1-1. GeoComm offers NG 9-1-1 specific software and services, including NG 9-1-1 GIS data assessment and development; GIS workflow consulting; software to maintain, manage, and provision NG 9-1-1

GIS data; the ECRF/LVF elements of the ESInet ; and tactical mapping for emergency responders and 9-1-1 Centers. GeoComm's solutions provide the tools necessary to geospatially route 9-1-1 calls, speed and enhance emergency response, improve data accuracy and quality, accelerate communications, and provide mission critical GIS-based decision support. GeoComm was first to demonstrate geospatial wireless call routing in 1999 at the APCO International Conference in Minneapolis, MN. This ground-breaking experience has helped shape the GeoComm NG 9-1-1 solutions portfolio and makes GeoComm the most experienced solutions provider in the industry today.

GeoComm's NG 9-1-1 products and services have been delivered to states across the country, including Maine, New York, Vermont, North Carolina, Pennsylvania, North Dakota, South Dakota, Iowa, Kansas, Texas, California, and Washington. In each case, GeoComm's dedicated team of GIS and Implementation professionals worked to achieve NG 9-1-1 GIS data readiness across the state.

GeoComm is actively involved in the following 9-1-1 associations:

Association/Influencers	GeoComm Involvement
Association of Public Safety Communication Officials (APCO)	Participation as an exhibitor and presenter at the annual conference. Attendance at the Emerging Technology Forum. GeoComm staff members serve on State Level Executive Boards and function as the Chapter Commercial Advisory Member (CCAM).
Esri	In March 2011, GeoComm became an Esri Platinum Tier Partner. Platinum Tier Partners, the highest of three tiers in the partner network, are recognized for developing and delivering industry-leading GIS solutions and services on the ArcGIS software platform. As a Platinum Tier Partner, GeoComm maintains a high level of collaboration with Esri and allows us to be involved with the direction for their future product development. Through the Esri Platinum Partner, GeoComm is involved with the Esri Partner Conference, Esri User Conference, Business Partner Conference, Developer's Conference, National Security Public Safety Summit, Technical and Business Meetings, Regional GIS meetings, and CTO Committee.
iCERT (Industry Council for Emergency Response Technologies)	GeoComm has been an iCERT member since 2009. GeoComm serves on the Innovation and Technology Committee. GeoComm's involvement in iCERT supports efforts to: • Assure adequate funding for 9-1-1 • Conduct scientific research which benefits the public by implementing improved emergency response technology • Bring together industry leaders to maximize the value of research and development investment • Represent the industry before the public and governmental bodies • Work with officials from organizations such as the NENA, National Association of State 9-1-1 Administrators (NASNA), and APCO

NENA
 	
(National Emergency Number Association)
	• NENA member
	• NENA Next Generation Partner Program member
	• Participation as a presenter and attendee of NENA's 9-1-1 Goes to Washington, Joint committee meeting, and Standards and Best Practice Conference
	• Participation as an exhibitor and presenter at the annual conference GeoComm has participated in, tested software, led, and co-organized multiple NENA sponsored Industry Collaboration Events (ICE).
	• Member of several past and current NENA workgroups, including:
	  ○ Site Structure Address Point Workgroup Participant
	  ○ GIS Data Stewardship for NG9-1-1 Workgroup Participant
	  ○ GIS Stewardship for NG9-1-1: Road Centerlines WG Participant
	  ○ DM-GIS Stewardship for NG9-1-1 Emergency Service Boundaries Co-chair
	  ○ PSAP Logistics – Request for Proposals Co-chair
	  ○ GIS Data Transition Co-chair
	  ○ ECRF/LVF Workgroup Chair
	  ○ Additional Data Workgroup Co-chair

Association/Influencers	GeoComm Involvement
	○ GIS Data Model for NG9-1-1 Workgroup Participant ○ NG9-1-1 GIS Data Model Standard v.2 workgroup co-chair ○ NG9-1-1 PSAP Systems Workgroup Participant ○ NG9-1-1 i3 Architecture Workgroup Participant ○ NG9-1-1 Management Considerations for Emergency Incident Data Document (EIDD) Interoperability Joint NENA/APCO Workgroup Participant
NG9-1-1 Institute	GeoComm is a Bronze NG9-1-1 Institute Supporter. GeoComm attends the Technology Showcase and 9-1-1 Honor Awards and serves on the Events Committee.
NSGIC (National States Geographic Information Council)	GeoComm is a Gold NSGIC Sponsor. GeoComm has worked with NSGIC to provide educational webinars to the NSGIC membership and attends the Annual Conference, Midyear conference, and serves on the NG9-1-1 Committee.
URISA (Urban and Reginal Information Systems Association)	GeoComm attends and presents at the GIS-Pro Conferences. In addition, GeoComm has several staff members that serve on the NG9-1-1 Task Force. GeoComm is also working with URISA membership to create a workshop for the URISA GIS Pro 2020 conference that will address NG9-1-1 GIS topics such as addressing, industry standards, jurisdictional boundaries, and more.

GeoComm's industry association participation extends nationwide and into nearly every state NENA and/or APCO chapter. For example, GeoComm proudly support the Nebraska APCO/NENA Chapter and Territory Sales Manager, Stacen Gross, currently serves as the Chapter Commercial Advisory Member (CCAM).

This broad participation provides the company with not only specific local understanding, but allows us to synthesize a picture of GIS data requirements nationwide.

DDTI has developed and installed key components ensuring reliable and timely emergency call routing. Their NENA i3 compliant software includes an emergency call routing function (ECRF), location validation function (LVF), location database (LDB), spatial interface (SI), and master street address guide conversion service (MCS). In addition, they offer map display software providing location awareness for 9-1-1 dispatchers in over 1,000 PSAPs nationwide.

DDTI continues to work closely with NENA to develop standards and protocols for NG 9-1-1 and has participated in multiple NENA Industry Collaboration events (ICE). DDTI has been recognized by NENA with a certificate of appreciation for their contribution to the development of ECRF/LVF NENA i3 standards.

DDTI is a leading provider of geographic information system (GIS) services, including field GIS data collection and comprehensive GIS data validation and normalization services, which serve in the preparation of NG 9-1- 1 deployments. DDTI has provided support for the creation of the location-based response system (LBRS) road inventory and address inventory for the State of Ohio.

DDTI products are currently supporting significant NG 9-1-1 deployments in the Commonwealth of Massachusetts, National Capital Region in Maryland, state of Montana, and several counties in Ohio. Additionally, DDTI frequently works with CPE vendors to ensure their software interfaces effectively with NENA i3 compliant GIS datasets.

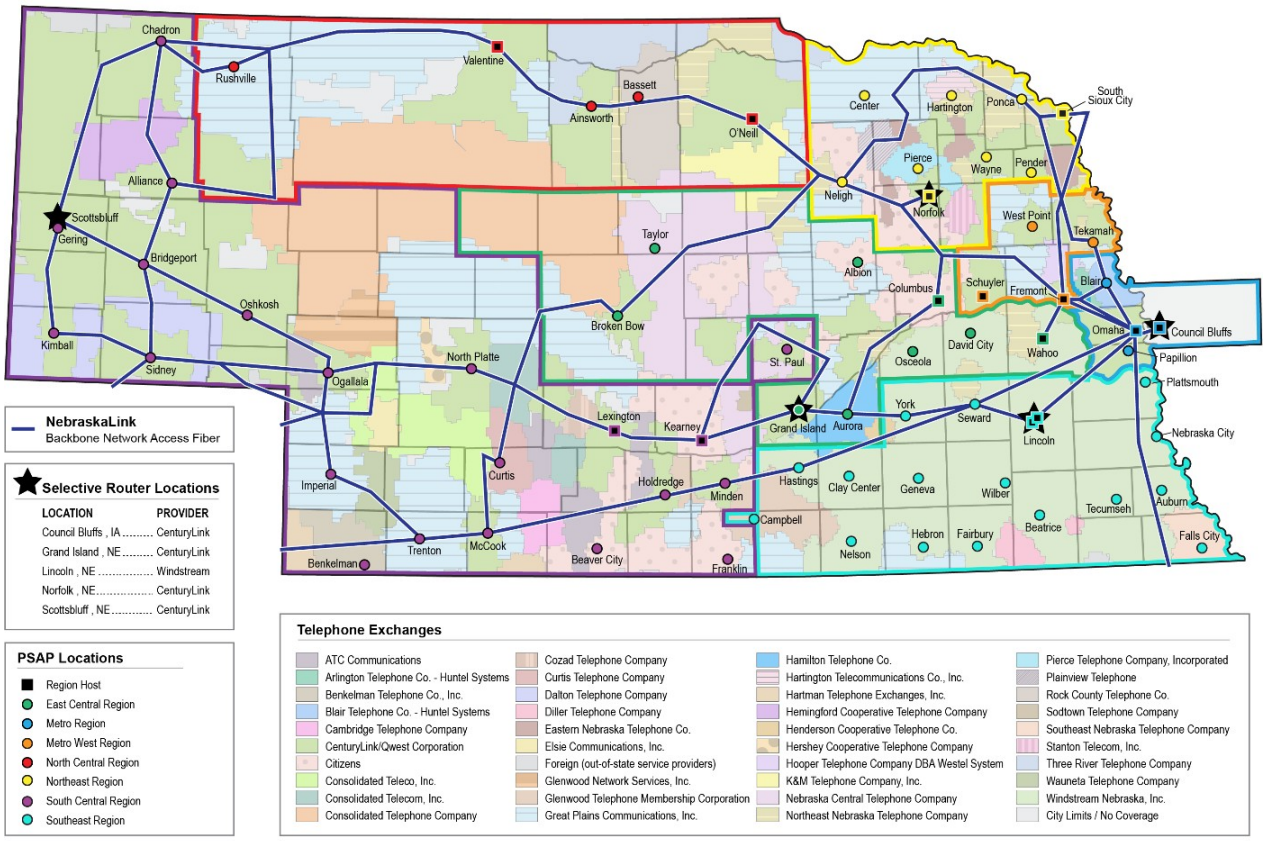
DDTI recently began a significant multi-year, multi-million-dollar contract with the State of Ohio Department of Transportation to provide support for the creation of the location-based response system (LBRS) road and address inventory. The U.S. Department of Transportation has specifically noted the accuracy of the LBRS data, as well as the collaboration of organizations required to build Ohio's LBRS, as this could serve as a model for the nation.

DDTI strongly believes in the consistent investment in product development and employee education, proving they have the necessary resources and capabilities to serve as a subcontractor for this project.

NebraskaLink is a statewide fiber optic network providing broadband transport and ethernet access across the state of Nebraska and beyond. NebraskaLink offers diverse, robust, and innovative solutions at competitive rates with an emphasis on provider-class internet connectivity and multi-site architecture. This infrastructure and investment allow for unparalleled service to the business community where high reliability and dependability are key. NebraskaLink is owned and operated in Nebraska, with Hamilton being one of five owners. The partnership between Hamilton and NebraskaLink has allowed Hamilton to expand its already broad infrastructure and data transport services. For the purpose of preparing this response,

NebraskaLink will provide Hamilton with all primary ingress and egress circuits, including their additional layer of NOC, and quality assurance services.

Nebraska PSAP/ILEC Map



iii. percentage of performance hours intended for each subcontract; and

The following information provides the percentage of performance hours intended for each subcontract.

Entity	Percentage of Performance Hours
INdigital	34.9%
GeoComm	12.8%
DDTI	6.9%
NebraskaLink	6.7%

iv. total percentage of subcontractor(s) performance hours.

The following information provides the total percentage of subcontractor's performance hours.

Entity	Percentage of Performance Hours
INdigital	34.9%
GeoComm	12.8%
DDTI	6.9%
NebraskaLink	6.7%

2. TECHNICAL APPROACH

The technical approach section of the Technical Proposal should consist of the following subsections:

a. Understanding of the project requirements;
b. Proposed development approach;
c. Attachment C - Technical Requirements Option A, B, and/or C;
d. Proposed high-level project plan
e. Schedule for the lifecycle of this project; and
f. Cost Proposal

Hamilton's response to technical requirements includes the following:

- A thorough understanding of the project requirements.
- Hamilton's proposed development approach.
- Separate responses for Attachment C – Technical Requirements Option B and C.
- A proposed high-level project plan.
- A proposed schedule for the lifecycle of Nebraska's NG 9-1-1 project.
- A separate cost proposal for each Attachment C – Technical Requirements (Option B and C).

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:	Hamilton NG911, Inc.
Bidder Address:	1006 12th St. Aurora, NE 68818
Contact Person & Title:	Jennifer Dennis
E-mail Address:	Jennifer.dennis@hamiltontel.com
Telephone Number (Office):	402-694-7235
Telephone Number (Cellular):	N/A
Fax Number:	402-694-5037

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:	Hamilton NG911, Inc.
Bidder Address:	1006 12th St. Aurora, NE 68818
Contact Person & Title:	Ryan Wineteer
E-mail Address:	Ryan.wineteer@hamiltontel.com
Telephone Number (Office):	402-694-7317
Telephone Number (Cellular):	402-631-9654
Fax Number:	402-694-5037

Form B
Notification of Intent to Attend Pre-Proposal Conference
Request for Proposal Number 6264 Z1

Bidder Name:	Hamilton NG911, Inc.
Bidder Address:	1006 12th St. Aurora, NE 68818
Contact Person:	Ryan Wineteer
E-mail Address:	Ryan.wineteer@hamiltontel.com
Telephone Number:	(402) 694-7317
Fax Number:	
Number of Attendees:	

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.

ATTACHMENT C — TECHNICAL REQUIREMENTS OPTION C

Bidders are instructed to complete a Matrix for Emergency Services Internet Protocol (IP) network (ESInet). 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 the 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.

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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement GEN-1.				

Any additional documentation can be inserted here:

Hamilton understands and can clearly demonstrate how its proposed solution aligns with NENA's i3 standard. Hamilton fully supports and monitors evolving standards and Hamilton has been highly involved in standards development through its active participation in NENA's Industry Collaboration Events (ICE).

COMPANY VISION

General Vision Statement

Hamilton fully understands that NG 9-1-1 is more than just a technology solution. First and foremost, NG 9-1-1 is a public safety medium that enables life-saving services to be delivered throughout Nebraska. For this reason, it is imperative that any solution be provided and performed in a coordinated phased approach, minimizing the disruption to live PSAP operations. The Hamilton team is comprised of individuals that have a tremendous knowledge of public safety requirements and are staffed with personnel who have, cumulatively, provided many, many years of service within the public safety industry.

Hamilton places emphasis on both compliance with standards and innovation, with the goal of providing customers with a NENA i3 compliant next generation solution accommodating the advancements in modern communications technology. The Hamilton NG911 system not only fulfills the requirements of this RFP, but exceeds expectations in many areas, ensuring improved services to all Nebraska PSAPs. Hamilton consistently looks for ways to improve its service offering to meet the emerging needs of the emergency communications industry, from caller to carrier to public safety entities, while always maintaining a highly reliable, standards-based and collaborative approach.

Hamilton has a proven track record of developing reliable and proven solutions in emerging technologies. We build NENA compliant functional elements (FE) closely following the emerging i3, Internet Engineering Task Force (IETF), and other NG 9-1-1 standards. This system of real-time software components delivers a robust and reliable solution for E9-1-1, interim level 2 and emerging interim level 3 (i3) networks. Hamilton's track record of reliable and proven solutions is the basis of what we see developing in the future.

Concepts on the Hamilton FE innovation roadmap range from automatic identification (AI) bots to enhanced location technologies.

We are constantly developing new products and features that can help ensure reliable delivery, consistent interaction, improve location for dispatch, and serve critical emergency sessions. We foresee an increasing flow of call (and caller) associated data, including publicly available information about the cell phone owner, personally identifiable information (PII) the public has chosen to store in their mobile device, and other advances.

For the PSAP call taker/dispatcher position of the future, we see increasing situational awareness from social media and the availability of images and video that can be accessed by the agency. We also see additional incident data from the emergency incident data document (EIDD) and incident data exchange (IDX) standard from adjacent jurisdictions.

NG 9-1-1 is considered a converged multimedia solution. Hamilton will provide a robust and seamless integration of new types of media and location types not previously available using legacy technology.

This is an end-to-end picture starting at the need for transitional legacy integration, including reliable interoperation with previous generation technologies like TTY, and ending with full NG 9-1-1 solutions supporting Real-Time Text (RTT), message session relay protocol (MSRP), and video.

That is a complete picture of the NGCS of the future, whether it be preparing for IMS / VoLTE or the internet of things (IoT) origination networks. Within the contract period, we will see many types of devices becoming integrated into the emergency services infrastructure.

Advocacy

Innovation starts at advocacy. Hamilton is constantly at the forefront of standards development and state legislation and regulation reform. Hamilton strives to provide the expert support needed to many of our customers. Hamilton has been involved in several initiatives and continues to advocate and lobby for industry advances, such as accessibility and location accuracy.

Network / Virtualization / Orchestration

On the network roadmap, we see the continuing use of traffic engineering fundamentals for evolving networks. The growth and adoption of software-defined networking (SDN) and multiprotocol label switching (MPLS) brings the ability for NGCS software components to participate in the routing. These advanced IP architectures provide greater quality assurance for packet flows across an ESInet at the network layer.

Hamilton is researching and developing these concepts, which include protocols like resource reservation protocol (RSVP). Our research goal is the proactive use of SDN to provide even more resiliency and quality in providing NG 9-1-1 solutions.

Hamilton is a proponent of utilizing any type of network connection available to create a network of networks. This allows seamless rerouting in the event of transport network element (NE) issues. In the past, we have utilized multiple providers, and in many cases different technologies to create an 'always available' network.

Additionally, we see the use of FirstNet to provide additional survivability to network related issues. In this proposal, we highlight MEVO(+), Hamilton's disaster recovery platform, and 4G VPN connectivity as an approach to achieve additional survivability from our primary network providers.

Hamilton is actively researching and developing for the network functions virtualization (NFV) front. This emerging technology builds on the reliability of previous generations of computer hardware virtualized in software. NFV is the latest trend of telecom and technology in the cloud. NFV has specific value in NG 9-1-1, especially in NGCS, regarding orchestration and functional component scalability. Hamilton is striving to take the best from NFV and put the more valuable pieces together, so we can evolve the ESInet at a safe pace.

Cyber Security

Hamilton understands the cyber security environment is ever changing with new vectors, actors, and solutions that emerge. We have a dedicated cyber security staff and continue to evaluate partnerships with commercial and government cyber security focused organizations.

It is naïve to believe any entity is immune from cyber security events. These types of events happen to the largest worldwide companies. Prevention and protection are crucial, but perhaps equally important is the ability to identify, contain, and mitigate.

This will include:

- Identifying ways to further leverage Information Sharing and Analysis Center's (ISAC) to help augment cyber security threat detection and mitigation.
- Evolving utilization of 911 Logix data analytics and artificial intelligence (AI) in identification of risks.
- Improving models for monitoring credentials and what occur in the industry with implementation of Identity, Credential, and Access Management (ICAM).
- Involvement with the discussions and advancement of the Task Force on Optimal PSAP Architecture (TFOPA) Emergency Communications Cybersecurity Center (EC3) concept as it evolves on the industry and national fronts.
- Continued adoption of the deeper use and further integration of technologies supporting single sign-on (SSO) and management functional areas (MFA).
- Developing generalized contingency plans for customers and the typical threat vectors.
- Implementing assessments and penetration testing of live public safety systems proves difficult without creating liabilities. We will provide examples to accomplish this and limit the liabilities.

NGCS Functional Elements (FE)

Hamilton is proactive in the NENA standards development process for i3 and related standards. We are constantly tracking the evolution of the i3 standard and preparing the NGCS network element layer for the future.

The roadmap includes the incident data exchange (IDX) and other emerging functions needed for NG 9-1-1 and the use of emergency incident data document (EIDD). Hamilton's vision includes business rule engines using artificial intelligence (AI) to look at the incident, location, and status of resources within the network to make intelligent decisions pre- and post-dispatch.

Hamilton is actively participating in the development of hybrid device location technologies along with its partners. Currently available and evolving are NGCS location technologies integrated to supplemental data providers to help provide the needed high-quality routing and dispatch decisions reducing emergency response times.

Reporting / Recording

All of Hamilton's functional elements (FE) can participate in an i3 event logging deployment, but also include a more robust and complete logging river/stream model that can be used by applications needing more detail than what an i3 event logger provides.

The Hamilton "Consistent Logging Strategy" is made visible via our proposed 911 Logix platform which provides for full awareness and visualization of call flows and related data records. This solution goes well beyond that possible with minimal i3 event logs.

Detailed events happening within the NGCS are placed on a secure and reliable logging bus and distributed as needed throughout the ESInet. On our roadmap are more analytics and reporting capabilities for 911 Logix. Hamilton's "Consistent Logging Model" will add additional software integrations for details, providing greater awareness of NGCS events themselves.

Further development of 911 Logix will include expanding analytics to identify trends and leverage AI technology for real-time analysis. We are also looking at partner vendor applications that could participate on feeding the event bus with other detail about activity taking place within a public safety network.

911 Logix

Hamilton's analytics & visualization platform, 911 Logix, is an advanced reporting tool that allows for the aggregation of numerous source data and for the visualization, reporting, and trending of ingress content in a NG 9-1-1 network.

Visualization from the largest to the smallest of views, with the ability to partition and manage content in the appropriate containers, is a leap forward for making sense of NG 9-1-1.

The tool provides for access to the data from any device at any time. Users of the system have near real-time access to the system via VPN and multi-factor authentication. The reporting and data collection system provides a secure user ID login and password with the ability to enforce minimum password requirements and require password changes on a predetermined interval.

The reporting and data collection system supports role-based access:

- Allowing statewide users to have access to reports for the entire state.
- Allowing some users to have access to PSAP(s) report information only.
- Allowing other users to have both PSAP and ECD Manager level access to report information.
- Allowing functionality/data to show only to certain users and not to everyone.

The reporting and data collection system allows the scheduling of automatic report generation and delivery by email as attachments to one or more recipients in a format selected by the recipient.

The 911 Logix release plan and evolution are based on the customer requirements and access to critical data points to meet those requirements.

Specific to the emergency communication routing function/location validation function (ECRF/LVF), Hamilton and its subcontractor staff have been active in NENA and work on, or have worked on, many of the NG 9-1-1 working groups to further Hamilton and the industry's vision for the advancement in NG 9-1-1. Some of these working groups include:

- 911CS-911 Core Services Committee (NENA)
- 911CS-i3 Architecture WG (NENA)
- ICE 9 Planning Committee (NENA)
- ECRIT
- NENA Information Document for GIS Data Stewardship for Next Generation 9-1-1 (NG9-1-1) (Co- Chair) (NENA-INF-028.1-201x)
- NENA Request for Proposal Considerations Information Document (NENA-INF-021.1-201x)
- NENA Information Document for Location Validation Function Consistency (NENA-INF-027.1-2018)
- NENA Standard for NG9-1-1 GIS Data Model (NENA-STA-006.1-2018)
- Requirements for a National Forest Guide Information Document (NENA-INF-009.1-2014)
- NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1 (NENA-INF-014.1-2015)
- NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard (NEN-STA-004.2-201x)

Through work with NENA and Internet Engineering Task Force (IETF), Hamilton has served as a strong proponent of open standards and interoperability to enhance 9-1-1 services within the United States.

Hamilton's Industry Expert Team comprised of Hamilton, GeoComm, DDTI, and INdigital staff are active participants and contributors in standards creation and committees, industry associations, and work groups applicable to the delivery of NG 9-1-1 services. This ensures that product development commonly aligns with evolving NENA standards.

Hamilton's Industry Expert Team comprised of NG 9-1-1 subject matter staff regularly participates in NG 9-1-1 Industry Collaboration Event (ICE) sessions, which are monumental in developing standards and protocols, as well as demonstrating industry leading functionality and integration capabilities. The Industry Expert Team has participated in the following ICE events: ICE 3, ICE 4, ICE 5, ICE 6, ICE 7, and ICE 8. Many products that are part of the Hamilton solution have been tested at these past ICE events and the Industry Expert Team is actively participating in the planning stages for ICE 9, which will focus on cyber security. The Industry Expert Team has also participated in the European Emergency Number Association (EENA) coordinated testing conducted at the Sophia Antipolis, France, test rail in 2017.

Additionally, as thought-leaders in the industry, the Industry Expert Team is involved in a variety of different NENA working groups, such as the Security for NG 9-1-1 (NG-SEC) Working Group, PSAP Guidelines for RTT Working Group, the NENA Operations/Logistics RTT Working Group, the Communication Modalities Working Group, the Emergency Notification for People with Disabilities Working Group, the Accessibility Committee, and many more. Overall, involvement in these working groups and at ICE events ensures the Hamilton team and Nebraska have current intelligence on the development of vital standards and will incorporate any modifications and changes into our solution as they are developed. Compliance with known applicable standards at the time of system acceptance, as well as continual upgrades to the system as required, will ensure the Hamilton solution meets evolving standards for the duration of the contract.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement GEN-2.				

Any additional documentation can be inserted here:

Proprietary Standards

Hamilton is fully compliant with the state's proprietary solutions and standards and is not utilizing any proprietary standards, interfaces, or protocols in the proposed solution.

Patented Technology

In addition, Hamilton is not utilizing any patented technology in the proposed solution.

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 requirements in Section V.D.1.b. of the RFP.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement GEN-3.				

Any additional documentation can be inserted here:

Hamilton acknowledges the Commission's request for a Public Safety Grade Next Generation 9-1-1 System to include the design and deployment of interface functions and security measures complying with current NENA i3 requirements as established in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards for the NENA i3 Solution. Hamilton's proposed solution meets, and exceeds, the state's definition of Public Safety Grade detailed within Section V.D.1.b of the RFP.

Hamilton demonstrates its support for the NENA i3 standard and any other relevant standards by being actively involved with the development of many of these standards, through its involvement in a variety of different NENA working groups, as well as the testing of interoperability at many of the NENA Industry Collaboration Events (ICE).

GEN-4	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement GEN-4.				

Any additional documentation can be inserted here:

Hamilton is proposing a purpose-built NG 9-1-1 network and managed services solution to meet the performance and availability requirements dictated by the Commission and the capacity demands of the state of Nebraska. This capacity includes current and planned ESInet traffic and usage that occurs as a result of data sharing in, and between, all participating PSAPs. Overall, Hamilton's proposed solution includes both next generation core service (NGCS) nodes and an ESInet transport design that exceeds the total design capacity for the state. Hamilton intends to use NebraskaLink as the underlying transport network to provide connectivity to the Regional Call Hosts (RCH). Hamilton's relationship with NebraskaLink allows us to acquire and provision transport from all relevant local providers. IP connectivity will be scaled to meet the requirements of each RCH, but will not be less than 200Mbps at each RCH. Pricing options to increase bandwidth to 500Mbps or 1Gbps connections have been included.

The core NGCS nodes will be located in two datacenters which include the Hamilton datacenter located at its corporate headquarters in Aurora, NE, and the Nebraska Data Center (NDC) located in Omaha, NE. These two datacenters will provide redundancy for the core nodes. We are proposing that each RCH have redundant dedicated IP connections. The primary connection, as illustrated in the pricing document, is a layer 2 fiber-optic connection. A secondary connection at each call host will be established using either commodity internet service or wireless 4G/LTE connectivity. Provisioning service in this manner maximizes carrier diversity and reduces fault tolerances.

NGCS nodes process both voice and non-voice media. Each node is capable of processing over 1,000 simultaneous SIP sessions. Peak processing on a production system has been tested to 14,000 sessions per second. Therefore, the call processing nodes are capable of processing call loads much greater than the historical call volumes for Nebraska. In lab testing, the SIP:ME routing core has been shown capable of sustaining call loads greater than 50,000 calls per hour.

Overall, Hamilton commits to provide the required capacity needed to ensure compliance to the service level agreements (SLAs). Hamilton's NGCS nodes are scalable and have the capacity to far exceed the growth requirements of the project providing capacity and support for all potential core functions and applications, such as call-handling systems, CAD, logging, GIS data, streaming media, Real-Time Text (RTT), IP traffic, traffic management systems, communications systems, and incident management systems. Hamilton is also responsible for the network planning and forecasting and will engineer the ESInet capacities based on these requirements.

GEN-5	**Capacity - 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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement GEN-5.				

Any additional documentation can be inserted here:

Hamilton commits to provide the required capacity needs to transition additional PSAP functions to the systems and network. Hamilton's solution is designed and deployed in a way that is easily scalable and provides the capability to grow in both capacity and coverage without disruption in service.

Hamilton's solution design permits scalability as the NGCS nodes are deployed in a virtual machine (VM) environment, providing the ability to add resources as required. Software licensing is commonly based on the population of a state/region/municipality. For the purpose of this proposal, software licensing would be based on the population of the state of Nebraska.

Hamilton's preferred network design is to utilize the highest quality network providers in each core site, PSAP, or region to develop the most reliable network. Hamilton's use of NebraskaLink's statewide fiber network will allow us to maximize the reliability of our design and use the highest quality transport method to create an ESInet.

By utilizing border gateway protocol (BGP), bi-directional forwarding detection (BFD), and other open shortest path first (OSPF) routing protocols, we propose to create a self-healing, scalable network. If additional bandwidth or additional survivability is required, it is simple to add additional network connections.

The ESInet will use redundant 1Gbps connections between the data centers. The router ports on the core-to-core connections are 1Gbps capable and would not require a hardware change in the event of increased bandwidth requirements. Hamilton has not experienced capacity constraints for transport speeds in excess of 1Gbps for deployments of more than ten times the population and call volumes of Nebraska's current volumes. In addition, Hamilton is willing to increase the datacenter to datacenter circuit speeds, and the associated core hardware components, to match the growth of throughput requirements to the Regional Call Hosts (RCH) at no additional cost to the state.

Hamilton is also responsible for the network planning and forecasting and will engineer the ingress ESInet capacities based on these requirements.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SEC 1.				

Any additional documentation can be inserted here:

Cybersecurity

Hamilton recommends the deployment of a private core ESInet. Interconnection to "public" networks are established through the use of session border controllers (SBC), virtual public networks (VPN), and other security related ESInet functional elements.

In addition to physical security, Hamilton fully supports the recommendations and best practices highlighted in NENA document NG-SEC 75-001 and applicable standards listed in Section V.D.1 Table 1.

Hamilton has dedicated staff with expertise in network and cyber security. Cyber security is an environment that is ever-changing with new attack vectors, bad actors, and solutions emerging at an increasing frequency. This necessitates concerted systems and procedures to maintain an effective security posture and relationships with commercial and government cyber security-focused organizations.

Hamilton will ensure that physical protection policies and procedures are documented, as well as implemented, to ensure sensitive information as well as information system software, hardware, and media are physically secure through access control measures. The Hamilton solution ensures for the physical protection of all system resources containing sensitive information.

The proposed solution includes firewalls, border control functions (BCF), and the implementation of access control lists (ACL) at all transitional interface points, including ingress and egress. The firewalls and the transition points they protect will be monitored.

Change controls (CMP) are in place, which require work plans, approvals, testing, coordination, documentation, security risk assessment, etc. Modification made to an ACL or firewall would be considered and governed by this change control process.

The firewalls protect and monitor at layers 2-7. Layer 1, or the physical layer, will be protected by building security measures, such as restricting access and disabling unused ports.

Security Requirements and Standards

The configuration will be in line with industry best practices such as National Institute of Standards and Technology (NIST) standards and NENA's next generation 9-1-1 security (NG-SEC) standard, as well as the security requirements listed within Section V.D.1 Table 1 of the RFP. These security requirements apply equally to all components of the system requested through this RFP, including data centers, networking-housing structures, and regeneration sites and other buildings housing any element or device that is part of the overall system provided by Hamilton and its subcontractors.

BCFs will be employed on both the ingress and egress sides of the network. All unused physical ports, or access points, will be disabled during equipment commissioning. Further, Hamilton uses the NIST Special Publication 800-53 procedures to evaluate network inventory to then create security controls and associated procedures based on the levels of risk associated with the identified threat vectors.

Compliance with adopted ESInet security standards is a shared risk across all PSAPs connected to the ESInet. Hamilton will educate and recommend compliance with all security procedures.

At the data centers, the proposed solution includes service organization control (SOC) 2 Type 2 certified safety and security recommended standards, with 24x7x365 environmental monitoring; video monitoring; dual factor access control; fire suppression system; and individually locked equipment cabinets and cages.

Hamilton has included in the proposed solution an Authentication, Authorization and Accounting (AAA) platform that is integrated into all user interfaces (UI) or portals as presented for use within or outside the ESInet.

The firewall, monitoring, alerting and management information system (MIS) supports a multi-tenant platform with a dashboard function for visibility and control.

Hamilton is fully committed to the NENA i3 standard process and results but focuses first and foremost on the design and operation of a secure ESInet system.

At the Regional Call Hosts (RCH), the backroom equipment will include a lockable half rack for the routing and switching equipment.

In addition, the solution provides a 24x7x365 network operations center/security operations center (NOC/SOC) specializing in 9-1-1 service management. The NOC/SOC utilizes a comprehensive tool set of monitoring applications focused on bandwidth usage, memory usage, CPU usage, and services availability. These platforms for alarms and monitoring vary depending on function and system and include NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and other supporting log subsystems.

Dashboards are utilized to provide comprehensive visibility from all systems listed above. The systems mentioned above and the dashboarding allow for alarms and threshold settings to alert and notify. The notifications can be delivered via visual display, text or email.

System and network alarming are provided through both the monitoring platform and the core network and next generation core services (NGCS) event logging sub-systems. The output of these systems is part of our NOC/SOC oversight of the ESInet. Hamilton will work with the Commission to determine the content and frequency of reporting desired for security status and analytics.

Specific to cyber security attacks such as telephony denial of service (TDoS) and distributed denial of service (DDoS), Hamilton utilizes the Fortinet intrusion prevention systems (IPS) within the BCF functional element (FE). Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

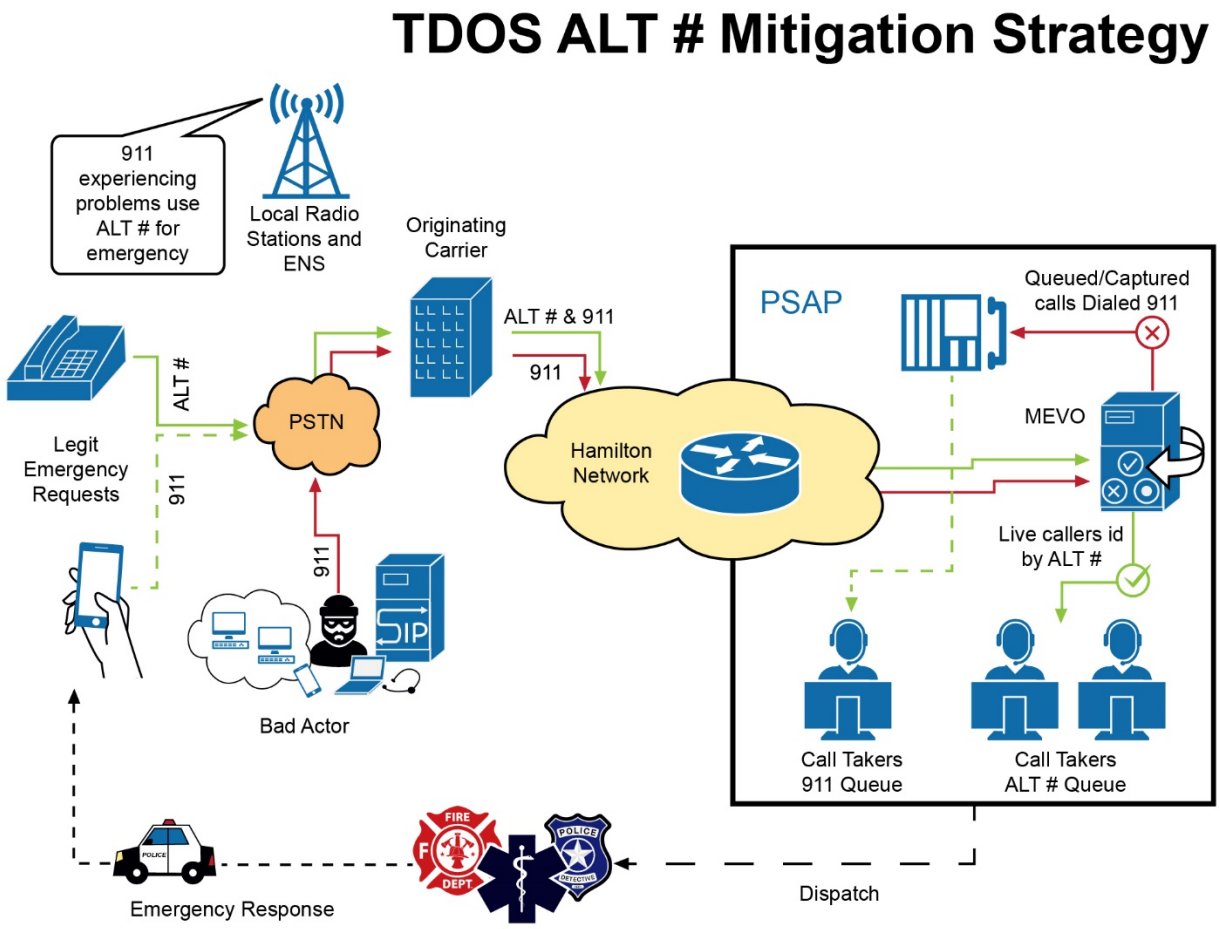
Telephony denial of service (TDoS) and distributed denial of service (DDoS) attacks can be difficult to identify, especially when originating from legacy OSPs, and require a multi-threaded process to mitigate associated vulnerabilities. Legacy network gateways (LNG) and session border controllers (SBC) are monitored with threshold detection to identify trunk saturation from the OSP network. Once alarmed, the NOC/SOC will actively identify the source, such as IP address, automatic number identification (ANI), or pseudo automatic number identification (pANI).

If a common source can be identified, it will be blacklisted, and an auto attendant will provide an alternate instruction, or customized delivery to the PSAP for emergency services. If the TDoS/DDoS attack cannot be isolated and live (good) calls cannot be distinguished from the TDoS/DDoS traffic, then other mitigation strategies will be implemented.

These other mitigation strategies vary by the nature of the intrusion and are not fully disclosed in a public facing document (such as this RFP response). They include implementing a honeypot in the call flow to attempt to gather more call location data; requiring a dual-tone multi-frequency (DTMF) response from the caller; using an alternate number; or utilizing an interactive voice response (IVR) system strategy.

As technology continues to advance, the ATIS 'SHAKEN' industry standard is expected to be more commonly available and will be evaluated.

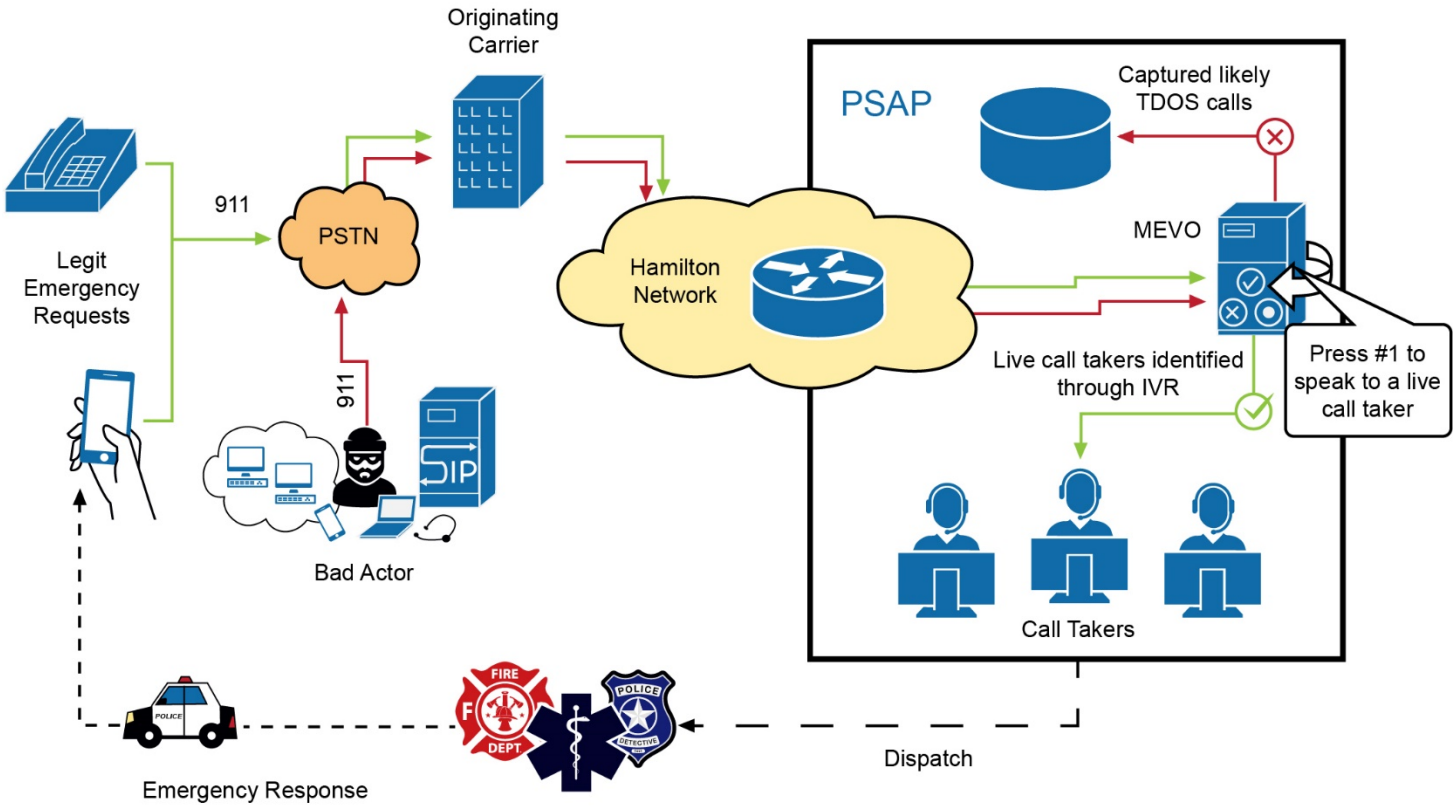
Hamilton has fully developed TDoS,DDoS, and Multimedia and Text Distributed Denial of Service (MTDDoS) action plans implemented in other NG deployments. These plans will be a component of the Nebraska implementation plan.



For example, one TDoS Alternate Number Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in a short time span) to listen to an IVR message. This IVR message directs the caller to contact an alternative 10-digit number for their emergency. All other callers are routed to 9-1-1 normally.

The TDoS IVR Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in short time span) to "press 1" to be connected to 9-1-1. All other callers are routed to 9-1-1 normally.

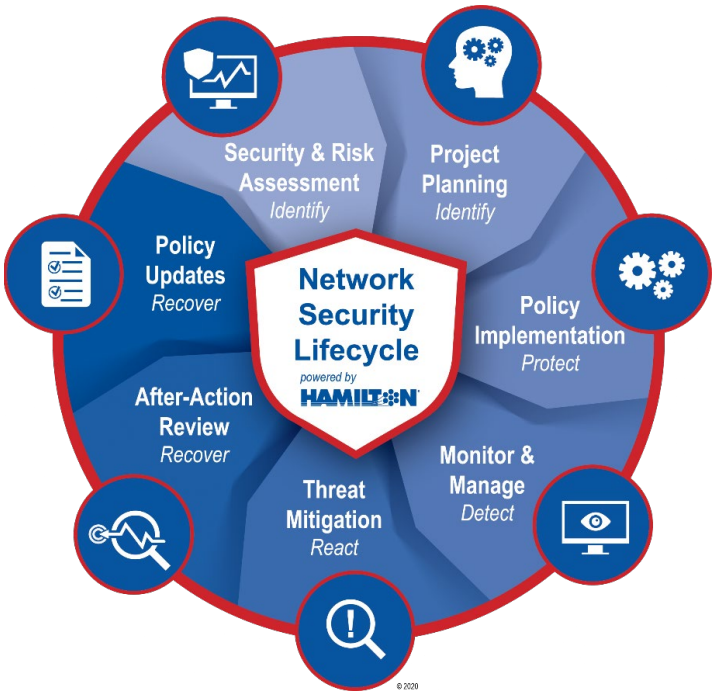
TDOS IVR Mitigation Strategy



For MTDDoS attacks, source IPs flagged as nuisance sources (multiple calls/texts in a short time span) will be filtered using blacklisting and whitelisting. Hamilton will work diligently to blacklist nuisance IP sources. However, if the bad traffic cannot be isolated, then the system will be set to send a bounce back message stating, "Text to 911 is not available at this time, call 911 for service." This will ensure those messages sent by individuals legitimately attempting to reach 9-1-1 by text message do not go unanswered.

At the conclusion of any cyber-attack, and upon resumption of normal operations, documentation of the event will be created. These documents include incident reports, tests completed, lessons learned, and service protections and improvements implemented.

Overall, security is an integral component of Hamilton's proposed solution and we have dedicated staff with expertise in network and cyber security. In addition, Hamilton continues to place concentrated attention on the development of several security items. In conclusion, the following points detail how Hamilton will monitor, detect, analyze, mitigate and respond to cyber threats and adversarial activity on the ESInet in alignment with applicable security standards contained within Section V.D.1:



- Identify ways to further leverage the Information Technology Information Sharing and Analysis Center (IT-ISAC) to help augment cyber security threat detection and mitigation.
- Utilize 911 Logix data analytics artificial intelligence in identification of risks.
- Employ Identity and Credential Access Management (ICAM) standards to create a model for establishing physical security procedures.
- Continued involvement in the advancement of the Task Force on Optimal PSAP Architecture (TFOPA) EC3 concept, as it evolves and becomes a national industry standard.
- Continued integration of technologies supporting Secure Sign On (SSO) and Multi-Factor Authentication (MFA).
- Conduct risk assessment analysis including the typical threat vectors.
- Perform physical security analysis.
- Develop contingency plans.
- Complete an assessment of all liabilities to be used in live testing scenarios. This will ensure the system is protected against real threats.

SEC 2	**Security Plan** A comprehensive security plan is a critical component of the Nebraska's NG911 network solution. Describe the security plan, including the 1. mitigation; 2. monitoring; 3. alerting and incident-response processes; and 4. 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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SEC 2.				

Any additional documentation can be inserted here:

Hamilton acknowledges the importance of a comprehensive security plan to the Nebraska NG 9-1-1 network solution and will develop a Security Plan specific to this proposed solution, Nebraska's requirements, and the results of the coordinated assessment per NIST 800-60 and 800-53 publications. Hamilton takes a holistic approach following the NIST Cyber Security and Risk Management and NENA's NG SEC frameworks using specifically the NIST 800-60 and 800-53 publications to evaluate an inventory of the systems and data used. Further, the plan will incorporate the latest NENA specifications and NIST 800-88 data-sanitization standards, the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) and Task Force on Optimal PSAP Architecture (TFOPA) best practices.

Nebraska's comprehensive security plan created by Hamilton and approved by the Commission will result in recommendations for the best controls to be implemented based on the levels of confidentiality, integrity, and availability required. This will result in a "living" plan. As the environment and system change, the plan will also need to adapt following the 3-tier method for assessing risk and the six-step security life cycle. Other requirements include reporting, auditing, incident procedures, frequency of tasks, etc.

As part of the Security Plan described above, a formal Incident Response Plan specific to the Nebraska NG 9-1-1 system will also be created, detailing the agreed upon structures. As part of the delivered solution, a Business Continuity Plan specific to the Nebraska solution will be created and tested annually for those systems that are capable of being tested without creating unwarranted risk to Nebraska's customers.

Mitigation

Suspicious activity that is identified by Nebraska, or by the Hamilton's employees or subcontractors, are initially reported to the network operations center/security operations center (NOC/SOC). Based on the information gathered from reports of end users and systems monitoring, the following steps are taken:

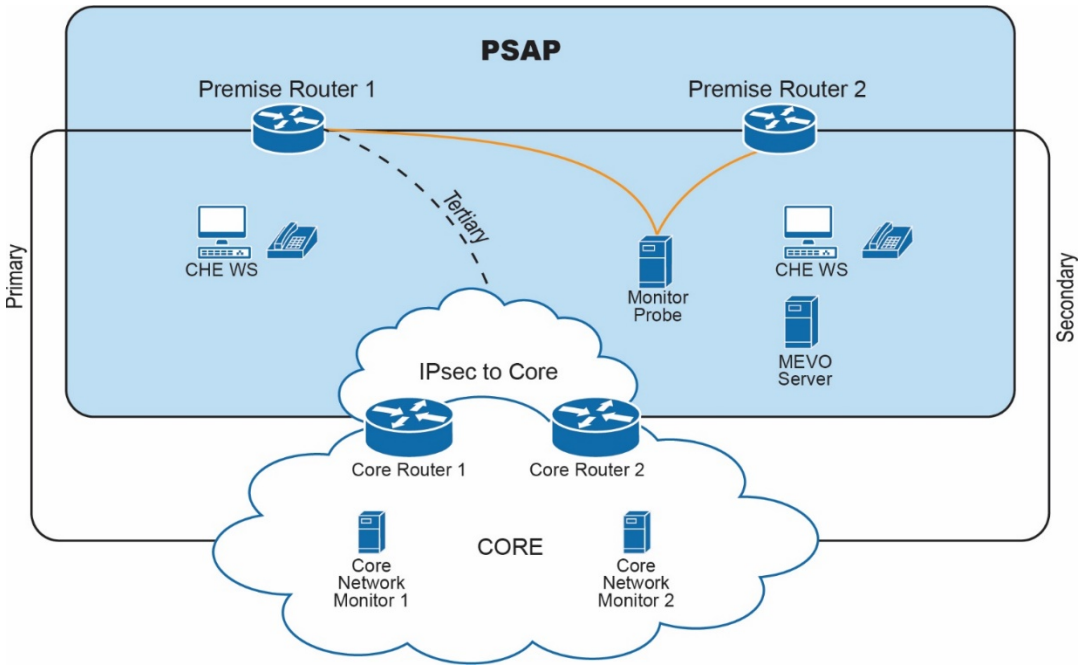
1. All suspected information security incidents must be reported promptly to the appointed Cyber Security Officer to speed with the assessment and identification of the breach, expedite any necessary mitigation, restoration and repair, and to facilitate the retention and gathering of any associated evidence.
2. Information security incidents must be reported to outside authorities whenever required to comply with legal requirements or regulations. Information relating to information security incidents may only be released by authorized persons.
3. All identified or suspected information security weaknesses require immediate notification of our Cyber Security Officer or a member of the management team.

Reports for any of the above breaches or incidents will be shared as mutually agreed upon with the state authorized designee.

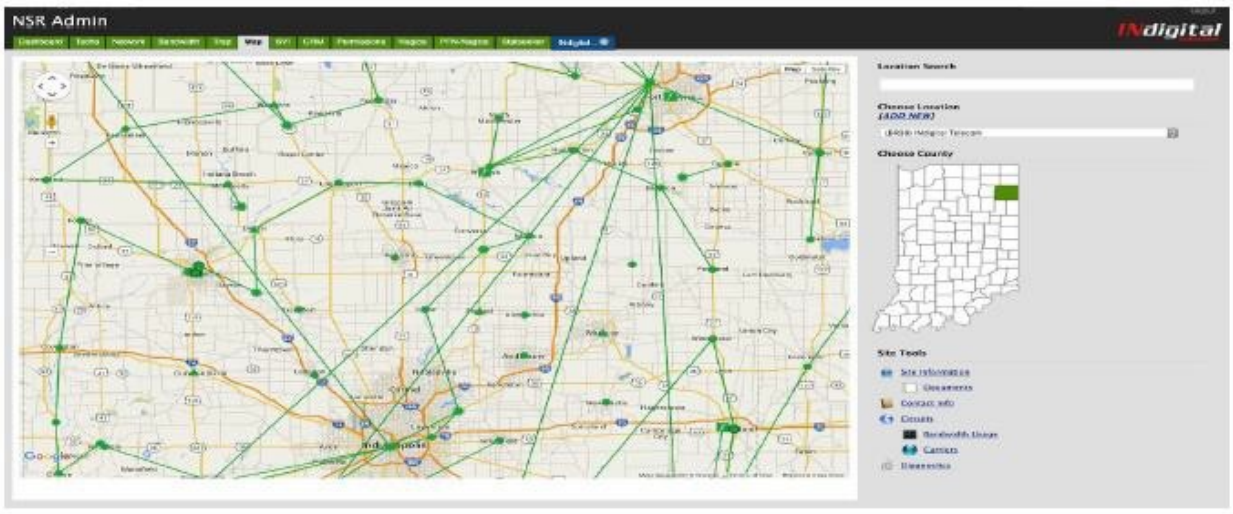
Monitoring

Hamilton provides an extensive system of monitoring systems. Much like NG 9-1-1 is a system of systems, so is the Hamilton monitoring suite of products. The monitoring system includes everything from bandwidth, trunking, application, resource management, system management, change control, and service level achievement.

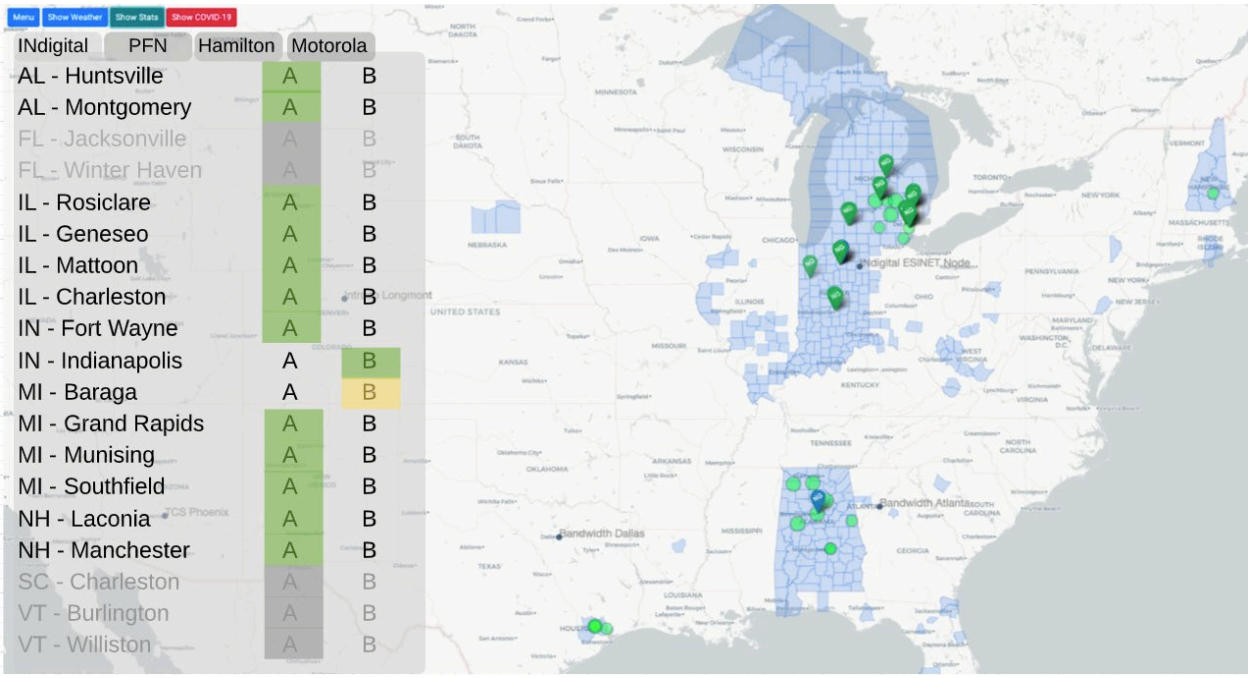
Unique to the Hamilton design of monitoring is the distributed probe approach. Not only is Hamilton monitoring from the core network, but also from the PSAP edge back into the network.



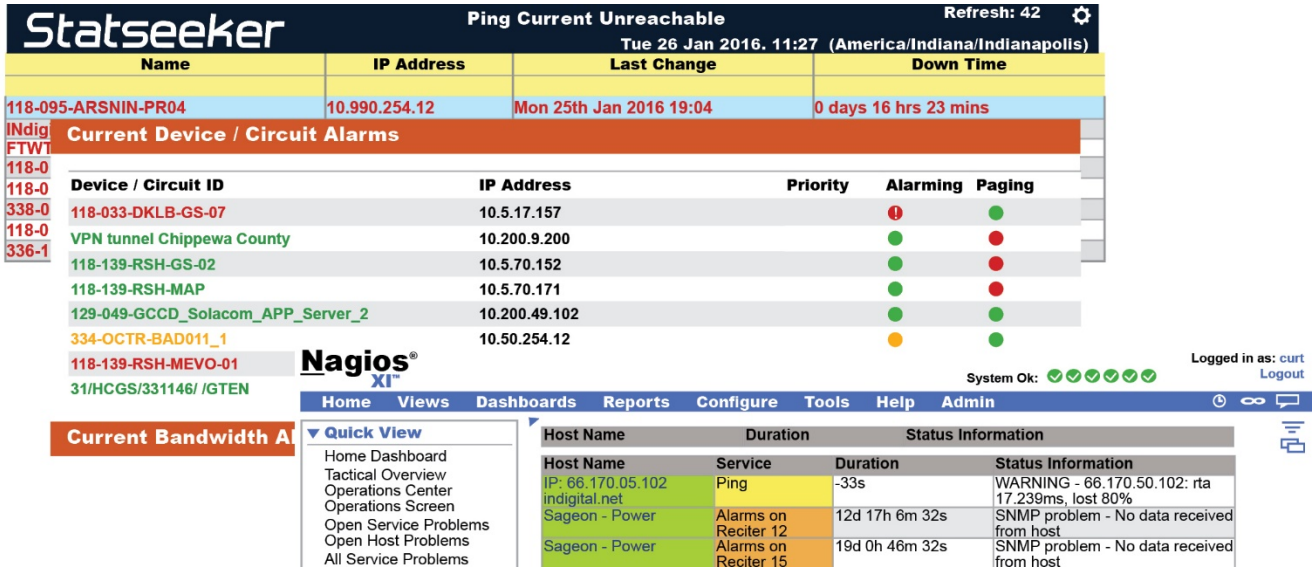
The use of monitoring probes at the edge of the network provides a full picture view of the service delivery at the PSAP, thus ensuring the highest levels of service at the PSAP.



Hamilton will provide the Commission with network status maps to display the health of the ESInet to all Nebraska stakeholders.

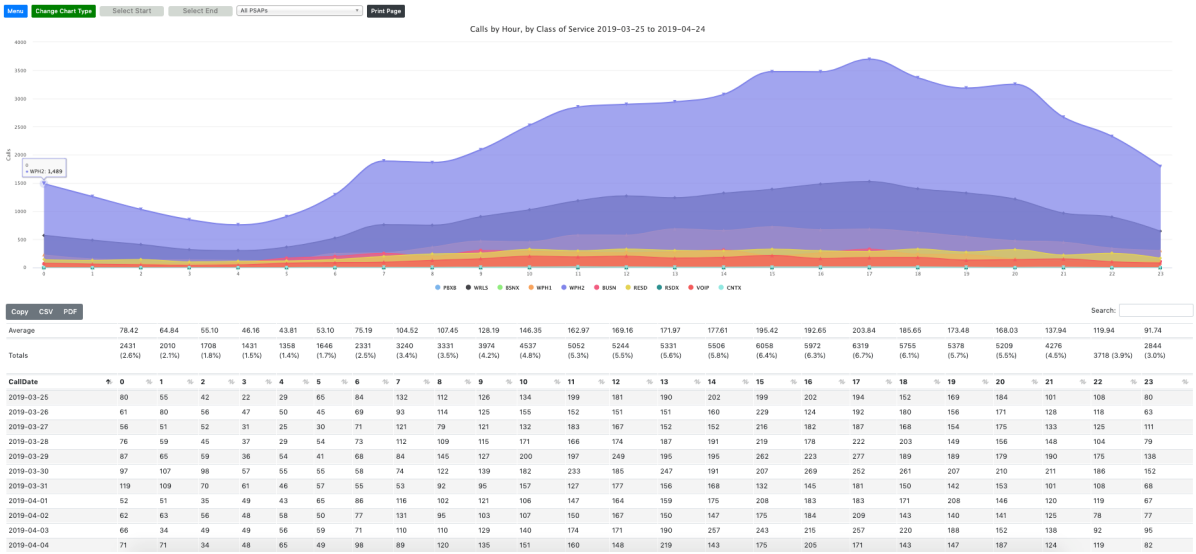


As referenced earlier, the proposed solution provides a 24x7x365 network operations center/security operations center (NOC/SOC) specializing in overall 9-1-1 management. This NOC/SOC utilizes a comprehensive tool set of monitoring applications, including NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and logging subsystems.



These various platforms each serve a different purpose, enabling Hamilton to provide a network utilization report to the Commission. This network utilization report will include the sizing of active networks and traffic volume trends.

Additionally, Hamilton will routinely complete audits of PSAPs and transport circuits, verifying records and maintaining physical and logical patch diversity relationships. The platforms listed earlier (i.e. NAGIOS, etc.) provide dashboards for comprehensive visibility and monitoring of the present state of the network, to include any loss in redundancy.



This image depicts a statewide activity view for call routing in the state of Alabama and provides an example for the state of Nebraska. The dashboard can be customized to include call data, trends, and threshold alarming. The system also provides the ability to collect and visualize NENA i3 logs from different systems such as next generation core services (NGCS), automatic location information (ALI), text-for-9-1-1, and CPE.

Alerting

The Hamilton monitoring system provides multiple layers of system alarming to Hamilton technicians and Nebraska stakeholders.

The various platforms used to monitor the present state of the network provide continuous visibility and monitoring. These consolidated dashboard overviews and detailed element statuses within the monitoring system will ensure abnormal traffic is immediately detected and customized alarms and threshold settings can be established, providing instant alerts and notifications via visual display, text, or email. Alarms are classified as follows:

- Critical
- Major
- Minor
- General Notice

These platforms can be utilized to provide the Commission with access to a network status dashboard allowing the proactive monitoring of systems, statistics and visualizations in near real time.

Alarming is through the monitoring platform, the core network, and next generation core services (NGCS) event logging sub-systems. The output of these systems is part of our NOC/SOC oversight of the ESInet. Hamilton will work with the Commission to determine the content and frequency of reporting desired security status and analytics.

Incident Response

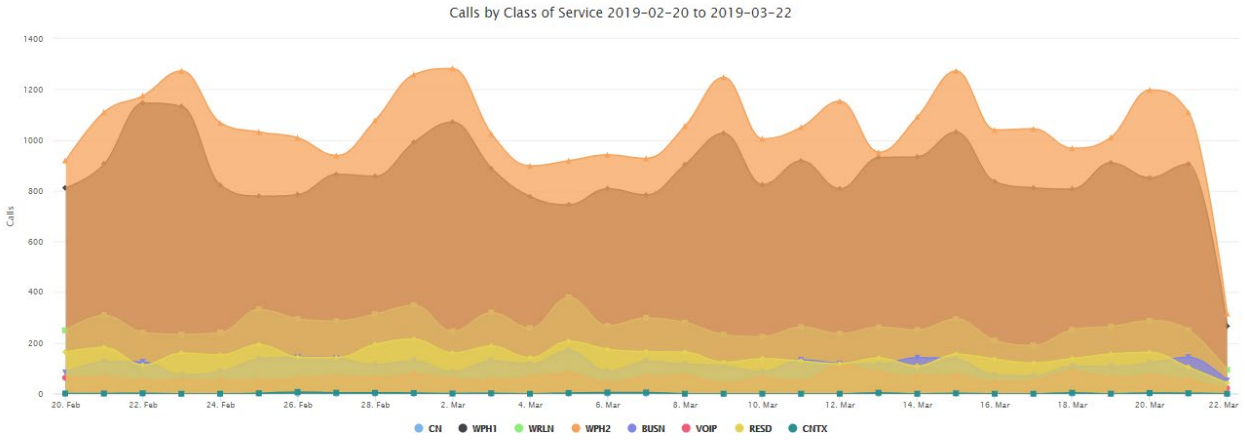
In the event of an unplanned outage, or intermittent outage of a system, network component, or application that has the potential to cause an adverse impact to production services, the various processes and procedures within the Incident Response Plan (referenced earlier as part of the Security Plan) will be referenced for dealing with various severity levels during the course of an incident. This Incident Response Plan will be created specific to this proposed solution, Nebraska's requirements, and the results of a thorough security assessment completed per industry standards. This plan will also detail the agreed upon service level agreements (SLA) and reporting structures.

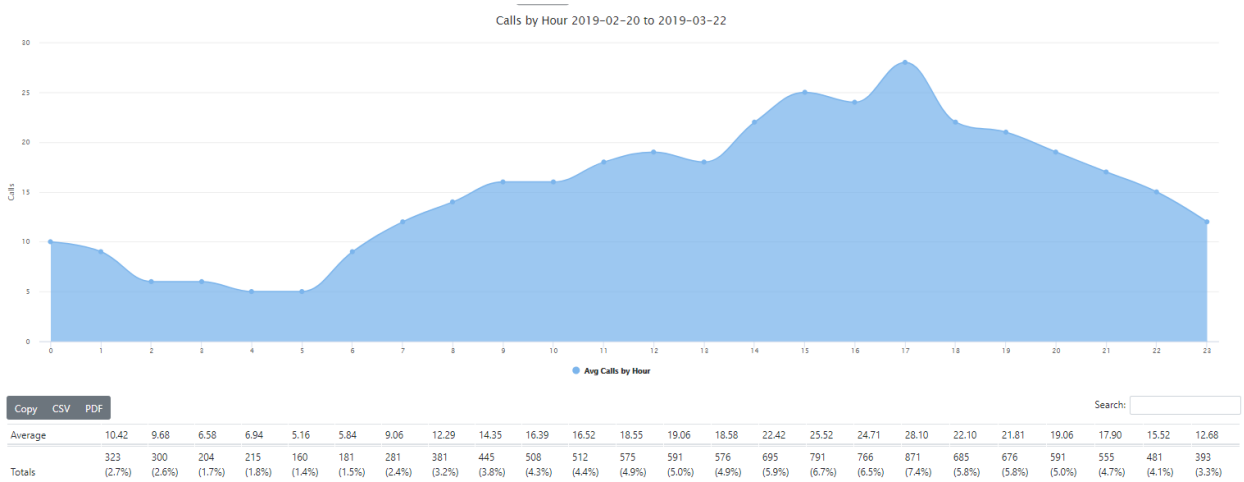
In conjunction with the solution's reliability, redundancy and diversity of the network, the requirements of FCC order 13-158 will also be met. Incident recovery will meet the NENA NG SEC standard of 50 miles from the normal operations location (NENA NG SEC section 7.5.5 Audit item # 213).

Logging

The solution proposed by Hamilton provides a comprehensive logging system and a dual factor secure reporting platform, which is accessible via a web portal called 911 Logix.

911 Logix includes access to the centralized logging system for all critical functional elements (FE) and CPE. This provides comparative analysis capabilities of network reporting vs. CPE reporting. Network reporting includes, but is not limited to, legacy network gateway (LNG), emergency service routing proxy (ESRP), automatic location identification (ALi), Text, MEVO(+) and threshold analysis. Examples are included below:





Average	10.42	9.68	6.58	6.94	5.16	5.84	9.06	12.29	14.35	16.39	16.52	18.55	19.06	18.58	22.42	25.52	24.71	28.10	22.10	21.81	19.06	17.90	15.52	12.68
Totals	323 (2.7%)	300 (2.6%)	204 (1.7%)	215 (1.8%)	160 (1.4%)	181 (1.5%)	281 (2.4%)	381 (3.2%)	445 (3.8%)	508 (4.3%)	512 (4.4%)	575 (4.9%)	591 (5.0%)	576 (4.9%)	695 (5.9%)	791 (6.7%)	766 (6.5%)	871 (7.4%)	685 (5.8%)	676 (5.8%)	591 (5.0%)	555 (4.7%)	481 (4.1%)	393 (3.3%)

SEC 3	**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.

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:

Hamilton complies with requirement SEC 3.

Any additional documentation can be inserted here:

Hamilton has completed the NENA NG-SEC Audit Checklist and it is attached as Appendix 6 – Hamilton NG-SEC Compliance Matrix. It is Hamilton's policy to update this Checklist on a quarterly basis. In addition, Hamilton has provided details within this response regarding the categories specified above.

Senior Management Statement: Hamilton's dedicated security staff has a Security Mission Statement that is approved by Hamilton's Senior Management. This Mission Statement clearly articulates the security mission of the company and the expectations of all involved in that effort.

Acceptable Use Policy: Hamilton has an established Acceptable Use Policy that clearly defines the acceptable use of Hamilton NG911 equipment.

Authentication/Password Policy: Hamilton authentication/password policy clearly and concisely explains password and authentication rules that follow industry best practices.

Data Protection: Hamilton accomplishes data protection through the policy of least privilege, backups, and encryption.

Exception Request/Risk Assessment: Exceptions to policy are requested through the Hamilton's established ticketing system, TeamSupport, and require approval by Senior Management.

Hiring Practices: Hiring practice include, but are not limited to, background checks, training, and signing of multiple policy forms to ensure compliance.

Incident Response: Hamilton has a fully developed and established Incident Response plan for corporate infrastructure and tailors an incident response plan for its clients based on their unique network and physical security environments.

Information Classification and Protection: All information is classified as either Public, Private, or Confidential based on the contents of the data.

Physical Security: Hamilton has implemented a robust and comprehensive physical security program and will implement a similar program for clients based on their unique physical security needs.

Compliance Audits & Reviews: Hamilton can perform compliance audits and reviews based on industry best practices specific to the 9-1-1 industry.

Network/Firewall/Remote Access: Hamilton has established policies to help mitigate the risk associated with network access, firewalls and remote access. These are enhanced by requiring different credentials for each mode of access.

Security Enhancement Technical Upgrade: Hamilton continuously reviews potential technical upgrades to enhance its overall security posture. This includes, but is not limited to, training, equipment upgrades, and policy updating.

Technical Solutions Standards: Hamilton continuously evaluates new technical solutions and measures them against their effectiveness in real world environments. Deep vetting occurs before the implementation

Wireless Security: Hamilton suggests keeping production 9-1-1 systems segregated from any wireless networks. In the event a production network needs to be integrated with a wireless network, industry best practice controls will be implemented to mitigate the risk associated with such a topology.

Overall, Hamilton has demonstrated its compliance with the identified requirements above contained within the NENA NG-SEC Audit Checklist. In addition, Hamilton has included within this response its completed NENA NG-SEC Audit Checklist in its entirety proving Hamilton's commitment to compliance with industry security standards. Please see Appendix 6 – Hamilton NG-SEC Compliance Matrix.

SEC 4	**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			
	Bidder Response Hamilton complies with requirement SEC 4.				

Any additional documentation can be inserted here:

The solution proposed by Hamilton offers several monitoring functions to provide predictive analysis and modeling to combat security threats. The Fortinet products utilized will leverage artificial intelligence (AI) and machine learning through its threat intelligence back-end to power the threat detection capabilities that make up the FortiGuard services. This information will be shared across the Fortinet Security Fabric.

Additionally, Hamilton will leverage other monitoring and reporting information such as NetFlow, call statistics, etc. to establish baselines for normal operation. Agreed upon thresholds, both high and low, will be established for deviation from those baselines. If a threshold is met or breached, alerts and notification will be sent to the NOC/SOC for further investigation.

SEC 5	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SEC 5.				

Any additional documentation can be inserted here:

This requirement refers to NENA's PSAP Credentialing Authority (PCA). This is one of the functions per NENA-STA-010.2 not yet fully vetted or implemented by the industry. Hamilton believes that this is an area of the NENA standard that will be advanced by the NENA ICE-9 event focusing on cyber security. While this standard is not fully vetted, Hamilton believes that our solution is compliant with the standards as they are currently defined.

The solution proposed by Hamilton includes an Authentication, Authorization, and Accounting (AAA) platform that is integrated into all user interfaces (UI), or portals, that are established both within and outward facing from the proposed ESInet.

All equipment and methods proposed are capable of providing the required authentication using industry best practices. This includes directory method certification using x.509 security certificates and a certification authority. We are aware of NENA's efforts to create a credentialing authority and are supportive of this initiative

SEC 6	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SEC 6.	X			

Any additional documentation can be inserted here:

Hamilton will comply with allowing annual third-party security audits at the request and cost of the Commission. Based upon NIST 800-53, the NIST Cybersecurity framework, and 9-1-1 industry best practices, Hamilton will work alongside the Commission to ensure compliance with the industry's top security standards. Completing formal audits and assessments in order to obtain independent measures of Hamilton's internal security posture is already a routine procedure for Hamilton. This is a requirement that Hamilton has had to comply with in other NG 9-1-1 projects in other jurisdictions and Hamilton is willing to collaborate with the Commission during this process. Further, Hamilton accepts the opportunity to further validate our compliance with industry security standards and the completion of external third-party audits will ensure the integrity of security controls and may identify areas of potential improvement. Hamilton will work with the Commission to accommodate any type or frequency of audit it desires.

SEC 7	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SEC 7.				

Any additional documentation can be inserted here:

Hamilton's proposed solution provides physical security to include physical access monitoring and reporting. The Nebraska Data Center (NDC) and Hamilton's data center employ certified safety and security recommended standards, with 24x7x365 environmental monitoring; video monitoring; dual factor access control; fire suppression system; and individually locked equipment cabinets and/or cages.

At the PSAPs, physical security of the local networking equipment, such as the routing and switching equipment utilized for the optional MEVO(+) disaster recovery system, will rely on the underlying facility access controls. Hamilton will work to educate and encourage industry best practices to maintain site and network security.

Hamilton will ensure that physical protection policies and procedures are documented, as well as implemented, to ensure sensitive information, as well as information system software, hardware, and media are physically secure through access control measures. The Hamilton solution ensures for the physical protection of all system resources containing sensitive information.

	General Requirements – Network Operations Center (NOC)/Security Operations Center (SOC)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/SOC 1	**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.	X			
	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.	X			
	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 systems, 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: Hamilton complies with requirement NOC/SOC 1.				

Any additional documentation can be inserted here:

Centralized NOC/SOC

As mentioned throughout this proposal, Hamilton will provide a dedicated 24x7x365 network operations center/security operations center (NOC/SOC), specializing in 9-1-1 service management, which will serve as a single point of contact for all PSAPs, interconnecting parties, and Nebraska. Additionally, the Hamilton help desk is located in the same facility as the NOC/SOC, ensuring Nebraska with the benefit of reduced reaction time and improved communication as the help desk and NOC/SOC personnel will coordinate efforts and response actions. Hamilton will provide 24x7x365 support and maintenance of the solution for the full duration of the contract and the service will be delivered with, and managed, according to applicable service level agreements (SLA).

The primary NOC/SOC is located at a facility in Ft. Wayne, IN. In the event of that facility becoming inactive, those operations would be redirected and distributed between our Indianapolis, IN, facility and another facility also located in Ft. Wayne, IN.

Overall, Hamilton's NOC/SOC will provide 24x7x365 proactive and reactive operations, administration, maintenance, and provisioning that assures the highest reliability and visibility of Hamilton services and maintains the integrity of data collected.

NOC/SOC Interoperability

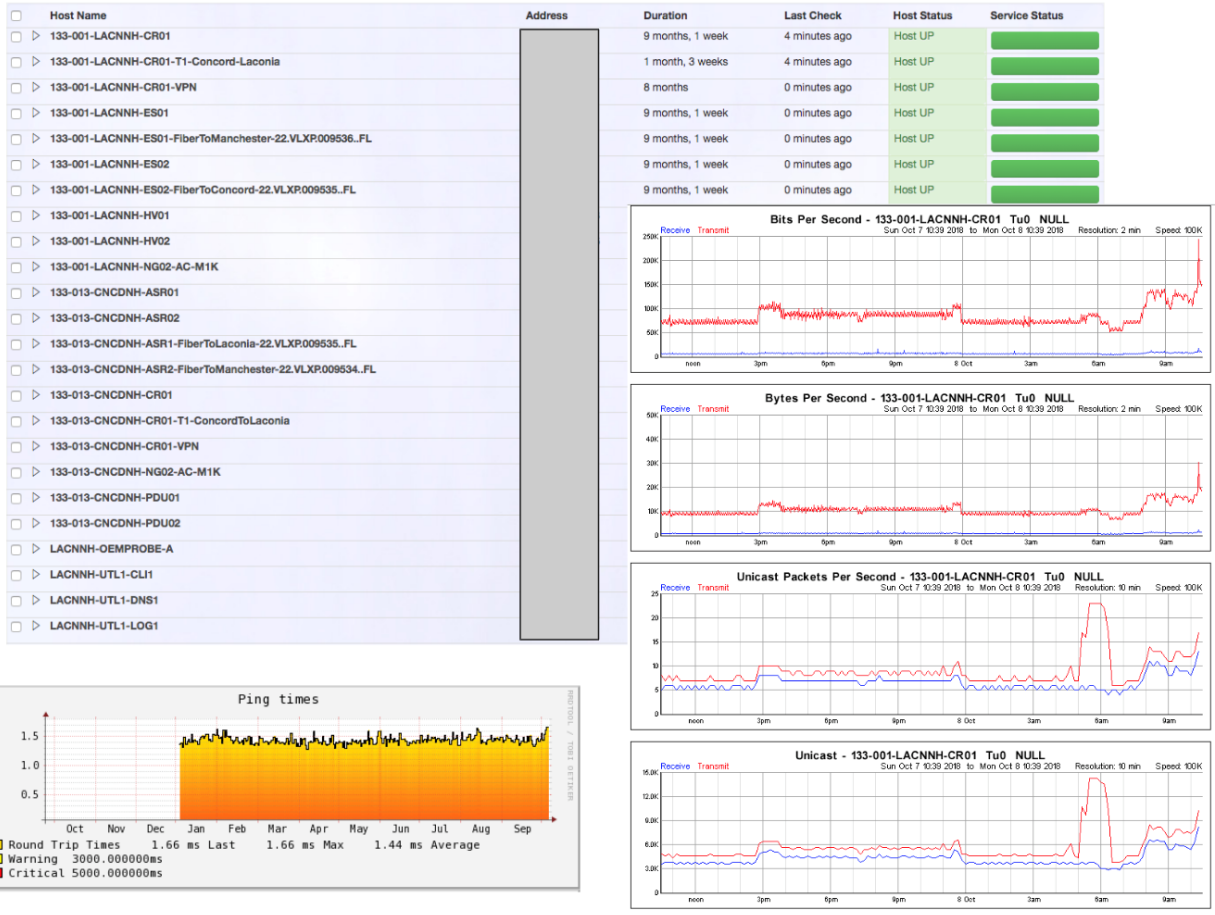
Hamilton's proposed solution can communicate, troubleshoot, and connect with other vendors' NOCs/SOCs should there be a different ESInet and NGCS provider. This will include interfacing with the NOCs/SOCs that support the regions through the state and the ebonding of ticket systems to support transparency throughout the troubleshooting process.

Hamilton's proposed solution will support eBonding in the IT Service Management (ITSM) platform. If Nebraska chooses to retain a separately contracted NOC/SOC provider to provide a single NOC/SOC view of the systems, Hamilton's NOC/SOC is capable of interfacing with other vendors. As detailed throughout this section, Hamilton's NOC/SOC is capable of interfacing with service providers and PSAPs utilizing a variety of communications means, such as text, email, and voice, to perform the tracking and notification functions on a 24x7x365 basis. Depending on Nebraska's decision for ESInet and NGCS providers (same provider vs. different providers), Hamilton's NOC/SOC is capable of supporting regional and/or state NG 9-1-1 networks, as well as providing a single interface for all NOC/SOC support regardless of Nebraska's deployment method.

NOC/SOC Operations Model

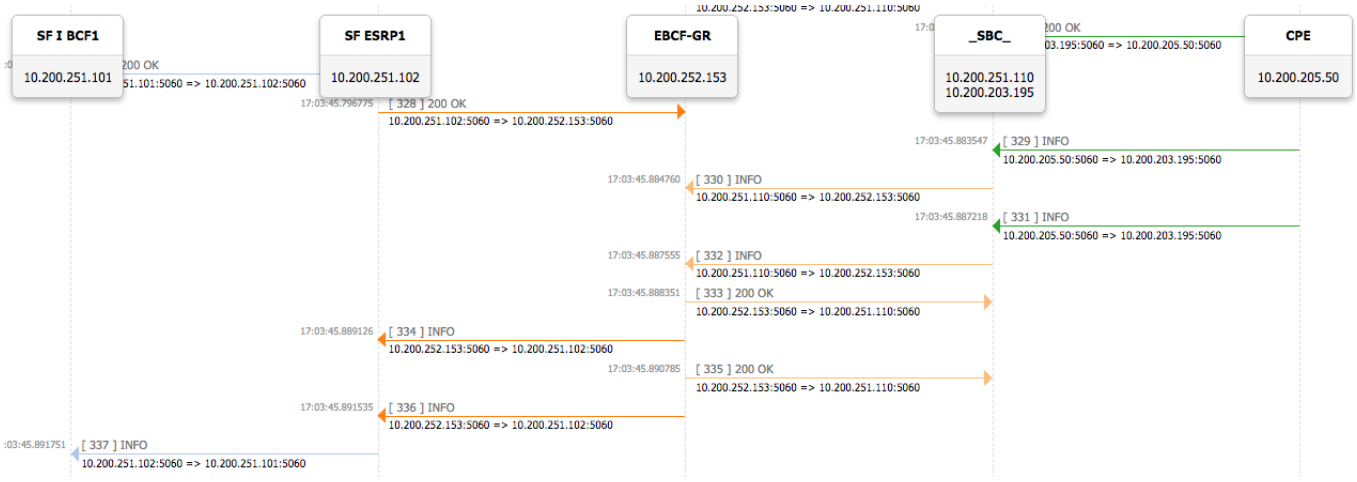
As mentioned within the centralized NOC/SOC section above, Hamilton's NOC/SOC operations model includes a dedicated 24x7x365 network operations center/security operations center (NOC/SOC), specializing in 9-1-1 service management, which will serve as a single point of contact for all PSAPs, interconnecting parties, and the Commission. Additionally, the Hamilton help desk will be located in the same facility as the NOC/SOC, ensuring Nebraska with the benefit of reduced reaction time and improved communication as the help desk and NOC/SOC personnel will coordinate efforts and response actions. Hamilton will provide 24x7x365 support and maintenance of the solution for the full duration of the contract and the service will be delivered with, and managed, according to applicable service level agreements (SLA).

A full portfolio of monitoring tools, such as NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and logging subsystems, as well as active alarming, are employed to identify potential problems before they occur. The NOC/SOC utilizes monitoring systems to log and alarm all facets of 9-1-1 services in near real time. This includes bandwidth usage, memory usage, CPU usage, and services availability. This includes all Hamilton devices in the core and PSAP.



The monitoring solution provides audio and visual alarming to the NOC/SOC. Alarms originating from critical applications and services notify appropriate engineers immediately and directly of possible problems.

Additionally, packet-level captures are collected within the core to provide the ability to recreate the session initiation protocol (SIP) call flow in a ladder diagram.

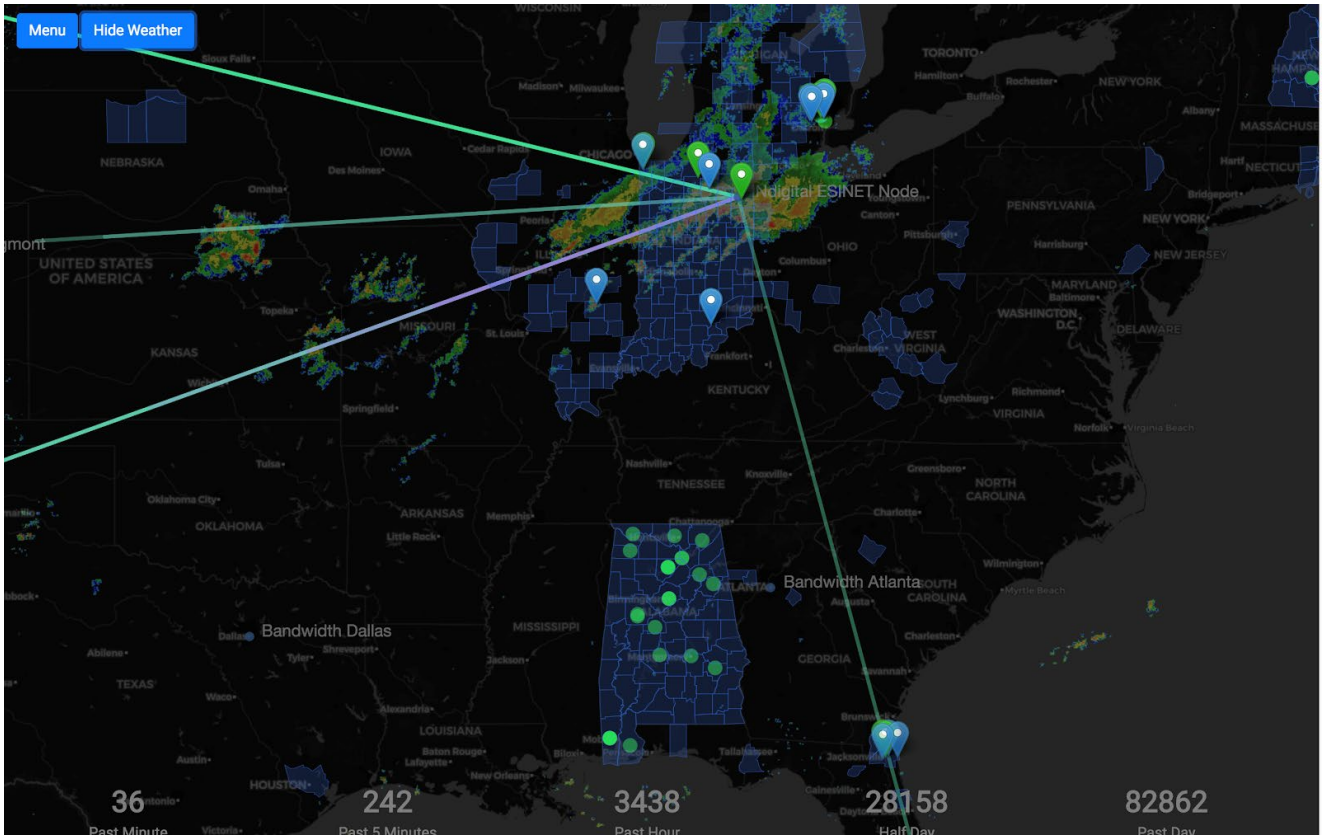


Tickets can be submitted via any of three methods. These include contacting the NOC/SOC through the toll-free phone number, email, or by utilizing the designated online trouble ticketing system.

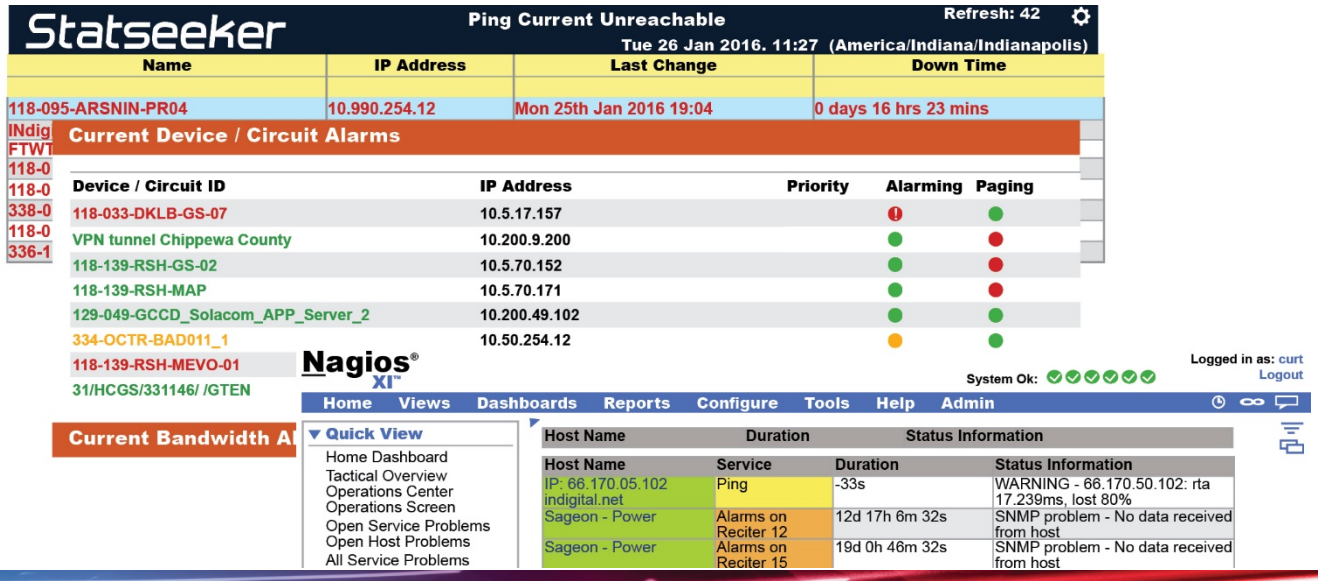
NOC/SOC personnel will ask a series of questions to help identify the severity of the problem, escalating to appropriate technicians as needed. Most general support issues can be resolved directly by NOC/SOC personnel.

Trouble tickets are created for every request to the NOC/SOC. Designated contacts are notified when a ticket is opened and will receive email notifications as the ticket is updated and resolved. Tickets of a more severe nature will prompt an immediate outbound phone call from the NOC/SOC to the designated recipients.

The solution also provides dashboards with comprehensive 9-1-1 call data with threshold alarming for next generation core services (NGCS) elements. These dashboards allow stakeholders to proactively monitor systems, statistics and visualizations in near real time.



The figure above captures a real time view of operations in the network. As a 9-1-1 service provider, it is important to have visibility of activities that are occurring in the network. This tool is above and beyond the traditional network management tools that are used by the majority of providers today. This allows Hamilton to see the impact of events that are taking place and impacting the PSAPs, while the network continues to operate as designed. Additionally, the NOC/SOC will have access and visibility into the security through the Forticloud and Fortiview functionality.



Suspicious activity identified by stakeholders, or Hamilton's employees or subcontractors, is initially reported to the NOC/SOC. Based on the evidence gathered from reports of end users and systems monitoring, the following steps are taken:

- All suspected information security incidents must be reported promptly to the appointed Cyber Security Officer to speed with the assessment and identification of the breach, expedite any necessary restoration and repair, and to facilitate the gathering of any associated evidence.
- Information security incidents must be reported to outside authorities whenever required to comply with legal requirements or regulations. Information relating to Information Security incidents may only be released by authorized persons.
- All identified or suspected Information Security weaknesses require immediate notification of our Cyber Security Officer or a member of the management team.

Reports for any of the above breaches or incidents will be shared as mutually agreed upon with the state authorized designee.

The primary NOC/SOC is located at a facility in Ft. Wayne, IN. In the event of that facility becoming inactive, those operations would be redirected and distributed between our Indianapolis, IN, facility and another facility also located in Ft. Wayne, IN.

Overall, Hamilton's NOC/SOC will provide proactive and reactive operations, administration, maintenance, and provisioning that assures the highest reliability and visibility of Hamilton services and maintains the integrity of data collected.

Continuity of Operations Plan (COOP)

Hamilton's proposed solution includes a defined continuity of operations plan (COOP). However, these guidelines are simply best practices for a COOP. A comprehensive evaluation of the customer site is necessary to implement the most efficient and responsive plan possible.

Hamilton's COOP ensures that all critical NG 9-1-1 services and NGCS functions can provide similar functions using alternative means in the wake of a disruption and after a disruption has been recognized. The COOP contains the following components:

- Facilities – As mentioned throughout this RFP, Hamilton's design foundation is comprised of diverse data centers, including the Nebraska Data Center and Hamilton's data center located at its corporate headquarters, providing geographic diversity. These facilities will operate in an active/active configuration. There are no hot sites, warm sites, and cold sites. All facilities are processing traffic and have the capabilities to handle all of the traffic for Nebraska providing true geographic redundancy and resiliency.
- Network - The ESInet that provides the foundation for the functional elements and transports the calls to the PSAP is redundant and resilient by design. Hamilton will provide redundant facilities and those facilities will be diverse by carrier where available. This prevents the service interruption due to transport provider network and technology.
- NGCS Functional Elements - The functional elements responsible for routing the 9-1-1 traffic for Nebraska has multiple layers of redundancy within itself.
    - Legacy network gateway (LNG) - Independent signaling system 7 (SS7) systems dual homed to active / active emergency service routing proxy (ESRP).
    - Interconnect border control function iBCF - redundant & mated to both ESRPs.
    - Egress border control function (eBCF) - Redundant & mated to both ESRPs.
- We will ensure there are safeguards to defend against exposure to any single point of failure and to ensure continuity of service.
- Additional and Alternate Technology - The proposed solution includes the optional MEVO(+) service as part of the continuity and disaster recovery system. MEVO(+) is designed to ensure delivery of calls and automatic location information (ALi) to the PSAP in the event of an impairment of the NGCS, ESInet or primary 9-1-1 call handling solution.

- The NGCS nodes use the policy routing function (PRF) to automatically reroute calls to the MEVO(+) system in the event of a system impairment or failure. This can also be accomplished at the individual PSAP level, at the regional level, or on a statewide level. Calls can be automatically re-routed to another PSAP, a mobile command center, or the MEVO(+) platform by the PRF function.
- Alternatively, PSAPs may request that calls be redirected to MEVO(+) by calling the network operations center/security operations center (NOC/SOC), or by activating the 'abandon PSAP switch' by the local authority. This is useful in accommodating scheduled maintenance activities at the PSAP. When calls are redirected to MEVO(+) at the PSAP level, MEVO(+) is deployed as a separate VoIP phone at each workstation. The phones are registered over the ESInet to the MEVO(+) server.
- If Nebraska opts to utilize the optional MEVO(+) service, specific PSAP Contingency Plans will be negotiated with each PSAP as part of the ESInet onboarding process. These plans will include action plans for PSAP busy scenarios, PSAP unavailable scenarios, bug out scenarios, or routine maintenance scenarios.
- MEVO(+) is further detailed throughout this RFP, including requirements NOC/SOC 22, SLA 18, and ESI 8.
- Personnel and Resource Planning – Hamilton's Industry Expert Team has many years of cumulative experience in the telecommunications industry. Further, the Hamilton team has a broad range of experience with a public safety focus and together, we continue to recruit and develop new talent to maintain and carry on our leading role in the industry.
- Cyber Planning and Response – With the transition from legacy methods and protocols to IP technologies, the continued planning for network security is a top priority for Hamilton. The security practices and continued risk management continue to evolve for NG 9-1-1 and our commitment is to demonstrate the reliability of our network services, as the threat profile changes for public safety. Our design enables the continuation of operations with the various cyber impacts to the network. The ability to assess, isolate, and mitigate the risk is key to the support of the service.
- Communication Plans - The Network operations center will be responsible for managing critical and routine events as they occur in the network. These events depending on scope will have various response criteria and communication plans. These responses may be from service restoration bridges for the dissemination and coordination of information to network service plans for maintenance upgrades during maintenance windows. Communication, planning and the sharing of information will be critical to the success for any event.

Additional information about Hamilton's COOP is provided in requirement NOC/SOC 22. The guidelines included within this RFP response are simply best practice for COOP. A comprehensive evaluation of the customer site is necessary to implement the most efficient and responsive plan possible.

In addition to the other components of Hamilton's COOP detailed within this response, Hamilton has an established pandemic response. This plan is actively and routinely reviewed by Hamilton's management team to insure it contains information that is both current and relevant. For more information on Hamilton's Pandemic/Infections Disease Plan, please see Appendix 7 – Pandemic/Infectious Disease Plan.

Problem & Change Management Systems

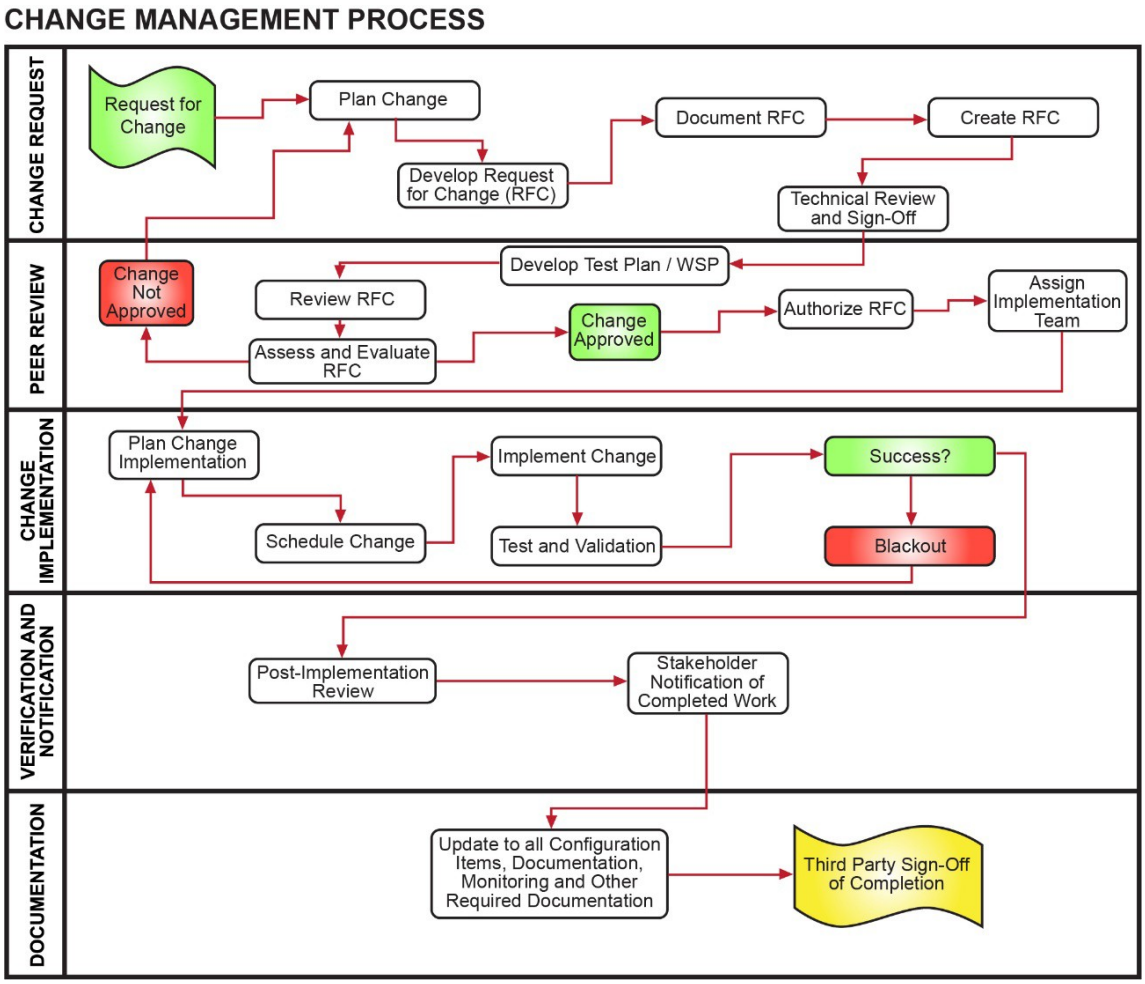
I. Planned Changed Management

Effective change management is of vital importance to emergency communications systems. If not managed correctly, changes introduce unnecessary risk. We manage this risk by following processes to help us analyze and plan the change, then implement the change in a controlled and considered manner. The complexity and rigor of the change management process depends on the magnitude and impact of the change. During the planning phase of the project, a Change Register Report (CRR) will be created specifically for the 9-1-1 Nebraska project and submitted for approval by the designated Nebraska NG 9-1-1 Project Manager.

All system changes require technicians to create a Change Management Process (CMP). The primary goal of the CMP is to require technical staff to create a plan, get technical sign off, document work, verify results, advise stakeholders of planned work and notify stakeholders upon completion.

After action reports (AAR) are a component of the CMP and are generated following all system changes, whether there was a negative impact to system performance or not. This allows for documentation of all pertinent information generated during system change processes.

All CMPs, including AARs, are made available to the customer. Please see the change management process in the figure below.



II. UNPLANNED CHANGE MANAGEMENT

Unplanned change events are typically emergency maintenance events. The same change control and maintenance notification processes utilized during planned events are also required as part of an unplanned event.

Notification to customers and other parties is required before any unplanned maintenance event. Notifications provide a summation of the work to be performed, along with an advisory as to the likeliness of the event causing an interruption in normal operations.

Work processes during an unplanned event are also required to follow similar procedures to a planned event. For example, a Maintenance Operation and Protocol (MOP) document must be created and approved by appropriate management prior to the completion of work.

The goal during an unplanned event is to ensure as much planning and communication is completed to ensure seamless call delivery.

Reporting Systems

Hamilton has a sophisticated notification policy that requires notification to end users and customers of many service impacting events. With 911 Logix, Hamilton is capable of providing the Commission, and any locally designated Regional Call Host (RCH) point of contact, with a report of all 9-1-1 calls that could not be delivered to a PSAP.

The Hamilton NOC/SOC serves as the central role as a source of status and additional information and uses a notification and reporting system that transmits voice calls, text messages, live chat, e-mail, and other methods of communication in an effective manner.

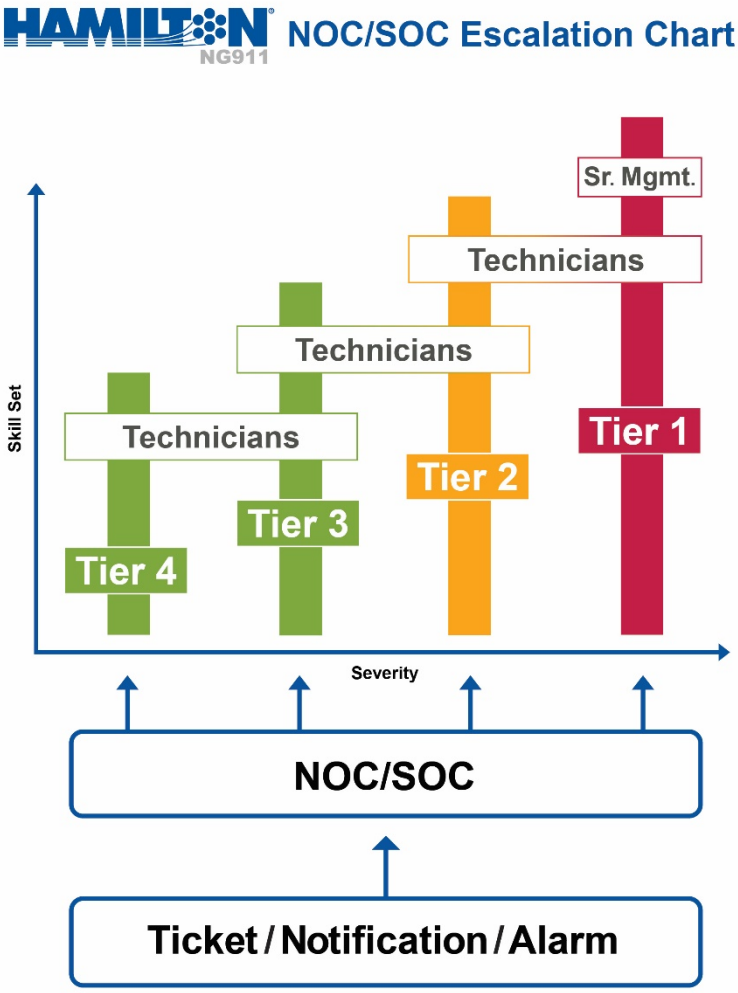
Hamilton also utilizes a trouble ticketing system that provides an audit trail and event updates to all parties in a transparent manner.

The trouble ticketing system provides updates to associated parties (e.g. PSAPs and other subscribed stakeholders) in near real time. In addition, Hamilton uses a mass notification method of e-mail and text messaging communication.

With the Hamilton NOC/SOC also functioning as a help desk, this ensures efficient resolution to open issues regardless of the situation.

Escalation Plan

The following diagram depicts Hamilton's established escalation procedures:



When a service ticket is submitted to Hamilton's NOC/SOC, it is classified and assigned based on severity. Hamilton's NOC/SOC is utilizing the following severity levels for classification:

- Tier 1 = Critical
- Tier 2 = Major
- Tier 3 = Minor
- Tier 4 = Maintenance

Depending on classification, service tickets are then assigned to appropriate staff. In the event of a tier 1 (critical) incident, or an outage scenario, senior management is automatically notified in addition to the appropriate technicians. If service issues could compromise service level agreements (SLA), staff will escalate to senior management via mass notification application. A pre-arranged outage voice bridge will be established to coordinate restoration efforts. Senior management has identified a Media Contact, specified in SLA 21, to execute the pre-defined media communications and stakeholder notification plan.

In the unlikely event of a malicious attack, the response team is expanded to the Executive, CTO, and Security Officer levels, who would be involved in developing and deploying a solution to resolve the issue.

In addition to the 24x7x365 NOC/SOC operation for support documentation and service-related issues, Hamilton provides an "In Case of Emergency" number to escalate critical services issues if the NOC/SOC were to be unreachable. Additionally, Hamilton provides an offsite call center that provides backup call support and escalation services.

Hamilton's escalation plan conforms with industry best practices. Hamilton follows the Information Technology Infrastructure Library (ITIL) for continuous service improvement as part of its organizational culture. Additional, Hamilton follows the National Institute of Standards and Technology (NIST) and NENA's next generation 9-1-1 security (NG-SEC) standards and best practices. The industry sees new actors and evolving vectors every day, thus our security posture takes a holistic approach always evolving to match with its environment. As the systems are changed and refined, this will be reflected in the supporting "living" documents.

Hamilton will provide a designated help desk for the Nebraska NG 9-1-1 project, acting as a central point for all communications for the PSAPs. The help desk will also serve as the Hamilton team's central point of contact for maintenance, warranty, and support operations; coordinating and facilitating communication among Hamilton's partners, subcontractors, vendors, equipment manufacturers, and any other entities involved in maintenance operations.

The Hamilton help desk will be in the same facility as the NOC/SOC, ensuring Nebraska with the benefit of reduced reaction time and improved communication as the help desk and NOC/SOC personnel will coordinate efforts and response actions. In addition to managing open tickets, the help desk can serve more broadly as Nebraska's customer service center, center of program operations, liaison between the PSAPs, technical staff, partners and vendors, and additional personnel involved in the project.

The help desk will open tickets for calls received using the existing, field-proven, ticketing system and provide the first tier of technical support by prioritizing, troubleshooting, and isolating problems. When required, the help desk will authorize and coordinate the dispatch of maintenance personnel and will escalate issues when appropriate.

Hamilton uses a variety of communications methods to ensure appropriate technical staff for escalations are notified. These methods of communication include typical telecom systems, as well as alarms and alerts through email, online messaging systems, and direct messaging software applications to provide internal mass notification.

Overall, Hamilton is very much aware that the escalation of problems is critical to the quality of service provided and is very much committed, and experienced, in providing suburb escalation and support services.

Conformance with Best Practices

Hamilton follows the Information Technology Infrastructure Library (ITIL) for continuous service improvement as part of its organizational culture. Additional, Hamilton follows the National Institute of Standards and Technology (NIST) and NENA's next generation 9-1-1 security (NG-SEC) standards and best practices. The industry sees new actors and evolving vectors every day, thus our security posture takes a holistic approach always evolving to match with its environment. As the systems are changed and refined, this will be reflected in the supporting "living" documents.

NOC/SOC 2	**NOC/SOC - Remote Connectivity Required** Contractor shall provide any network connectivity required to support Contractor's 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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NOC/SOC 2.				

Any additional documentation can be inserted here:

Hamilton will provide any network connectivity needed to support its NOC/SOC services.

Because of our experience in providing critical public safety services for over 50 years, Hamilton has the necessary expertise and capabilities to deliver support to our customers, ranging from full remote support to on-site operational responsibilities.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 3.				

Any additional documentation can be inserted here:

The proposed security architecture will control access to network resources according to the most current versions of 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. Hamilton's security management will comply with all security and data integrity standards listed in Section V.D.1. Table 1 of the RFP to monitor users logging into network resources and to refuse access to those who enter inappropriate access codes.

The proposed solution includes firewalls, border control functions (BCF), and the implementation of access control lists (ACL) at all transitional interface points, including ingress and egress. The firewalls, and the transition points they protect, will be monitored.

All access to a network has the potential to introduce malicious activity. Any and all remote access to the NG 9-1-1 system must adhere to security measures and policies intended to protect the system. The proposed solution includes two factors, one-time password, or session authentication, for all Internet-based services such as 911 Logix, PSAP Toolkit, and other public systems. The proposed solution complies with NENA's next generation security (NG-SEC) recommendations for all outward facing portals and interfaces. The following components make up the Hamilton solution's secure remote access capability:

Authentication Manager: The authentication manager server will provide an authentication service for RSA Smart Tokens, which will be provided to any remote users requiring any type of remote access to the NG 9-1-1 system. These Smart Tokens provide secure, two-factor authentication to the network. Once authenticated, a client VPN session is established to the firewall/VPN connected to the external Internet connection point.

Authorized Manufacturer Access: Escorted access for manufacturers will operate as a remote access gateway for the method of supporting manufacturer and vendor software and other configuration updates. After the live deployment into the NG 9-1-1 system, this access method will be audited and screened for compliant security and control.
Change controls (CMP) are in place, which require work plans, approvals, testing, coordination, documentation, security risk assessment, etc. Modification made to an ACL or firewall would be considered and governed by this change control process.

The configuration will be in line with industry best practices such as National Institute of Standards and Technology (NIST) and NENA's next generation 9-1-1 security (NG-SEC) standard. The firewalls protect and monitor at layers 2-7. Layer 1, or the physical layer, will be protected by building security measures, such as restricting access and disabling unused ports.

At the data centers, the proposed solution includes service organization control (SOC) 2 Type 2 certified safety and security recommended standards, with 24x7x365 environmental monitoring; video monitoring; dual factor access control; fire suppression system; and individually locked equipment cabinets and cages.

At the Regional Call Hosts, security will rely on the underlying facility physical access controls. The backroom equipment at these sites will include a lockable half rack for the routing and switching equipment.

The proposed solution's 24x7x365 NOC/SOC specializing in 9-1-1 service management utilizes a comprehensive tool set of monitoring applications focused on bandwidth usage, memory usage, CPU usage, and services availability. These platforms for alarms and monitoring vary depending on function and system and include NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and other supporting log subsystems.

Dashboards are utilized to provide comprehensive visibility from all systems listed above in real-time. The systems mentioned above and the dashboarding allow for alarms and threshold settings to alert and notify. The notifications can be delivered via visual display, text or email.

Hamilton has included in the proposed solution an Authentication, Authorization and Accounting (AAA) platform that is integrated into all user interfaces (UI) or portals as presented for use within or outside the ESInet.

The firewall, monitoring, alerting and management information system (MIS) supports a multi-tenant platform with a dashboard function for visibility and control. Alarming is through both the monitoring platform, the core network and next generation core services (NGCS) event logging sub-systems. The output of these systems is part of our NOC/SOC oversight of the ESInet. Hamilton will work with the Commission to determine the content and frequency of reporting desired for security status and analytics.

The proposed solution utilizes the Fortinet intrusion prevention systems (IPS) within the BCF functional element. Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

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. **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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
				X	
	Bidder Response: Hamilton complies with requirement NOC/SOC 4.				

Any additional documentation can be inserted here:

Connected Systems Compliance

Hamilton's proposed solution will comply with all standards listed in Table 1, including security standards. Hamilton commits to demonstrating its compliance and commitment to standards through participating in initial and recurring audit.

Hamilton's subcontractor, INdigital, is contractually obligated to perform annual SOC 2 Type 2 security audits. Additionally, INdigital has begun a third-party assessment with SecuLore to assess existing NOC/SOC systems and baseline security policies. SecuLore's "CyberBenchmark™" process implements Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) and Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) best practices. Results of the "CyberBenchmark™" assessment will be shared with Hamilton, in addition to updated policies and procedures which are expected as a result of the assessment.

This is being done as a predecessor to, and in preparation for, SSAE18 auditing. The intention of utilizing the SecuLore Overwatch™ solution is to fulfill the penetration testing requirement through continuous passive vulnerability assessments,

monitoring, logging and reporting. Additionally, this system provides the ability to capture the necessary information necessary to assist in recovery and forensics in the event of a cyber security event.

Security Reports and Recommendations

In accordance with the Commissions requirements, Hamilton will provide, within 30 days of the end of each calendar month, security summary reports and recommended improvements. These will include incidents and incident response; building, facility, and network access reports including failed attempts; identified and open software vulnerabilities with associated high/medium/low designations; and updates and/or changes to security systems and software. All related data will be retained for the period of the contract and provided to the Commission electronically at the end of the contract.

Hamilton maintains access logs for all functional elements. These logs will be included in the monthly reports provided to the Commission.

In addition, Hamilton will include security status reports as a part of its routine reporting portfolio. The Forticloud platform, a component of the proposed solution, is an integral part of Hamilton's security management system. This platform supports multi-tenant environments with a dashboard function for visibility and current status of the ESInet and its security state. Additional reporting can also be included as agreed upon by Hamilton and the Commission.

NOC/SOC 5	**NOC/SOC – Connected Systems Compliance 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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NOC/SOC 5.				

Any additional documentation can be inserted here:

Hamilton's subcontractor, Indigital, employs third party oversight by SecurLore. Their Paladin Overwatch™ service uses layer 2 network monitoring to provide predictive analysis. For example, by analyzing data packets in and out of the network, NOC/SOC personnel have been able to find and isolate ransomware before it spreads. This service is independent of the endpoint security solution in use.

The Cybershapes methodology will allow alerts generated at machine speed to be shaped and then easily viewed by the NOC/SOC. This will allow human aided artificial intelligence (AI) to determine an attack or vulnerability through early event analysis. This approach can be used to immediately isolate, contain, and even prevent attacks.

Hamilton provides several safeguards related to minimizing the effects of TDoS and DDoS attacks. The first safeguard includes a network intrusion detection and prevention (IDS/IPS) platform with distributed denial of service (DDoS) support. This first level defense is designed to prevent DDoS attacks. Further, our ESInet design limits exposure by keeping the ESInet private and segmenting firewalled touchpoints to the Internet or external domains.

Telephony denial of service (TDoS) prevention is handled in a similar way by managing the number of possible concurrent calls from the originating source and utilizing threshold monitoring to detect changes in normal call patterns. More advanced TDoS techniques are available for the separation of real 9-1-1 traffic as compared to spam traffic. These techniques use industry standard methods, as well as protocols that are trade secrets.

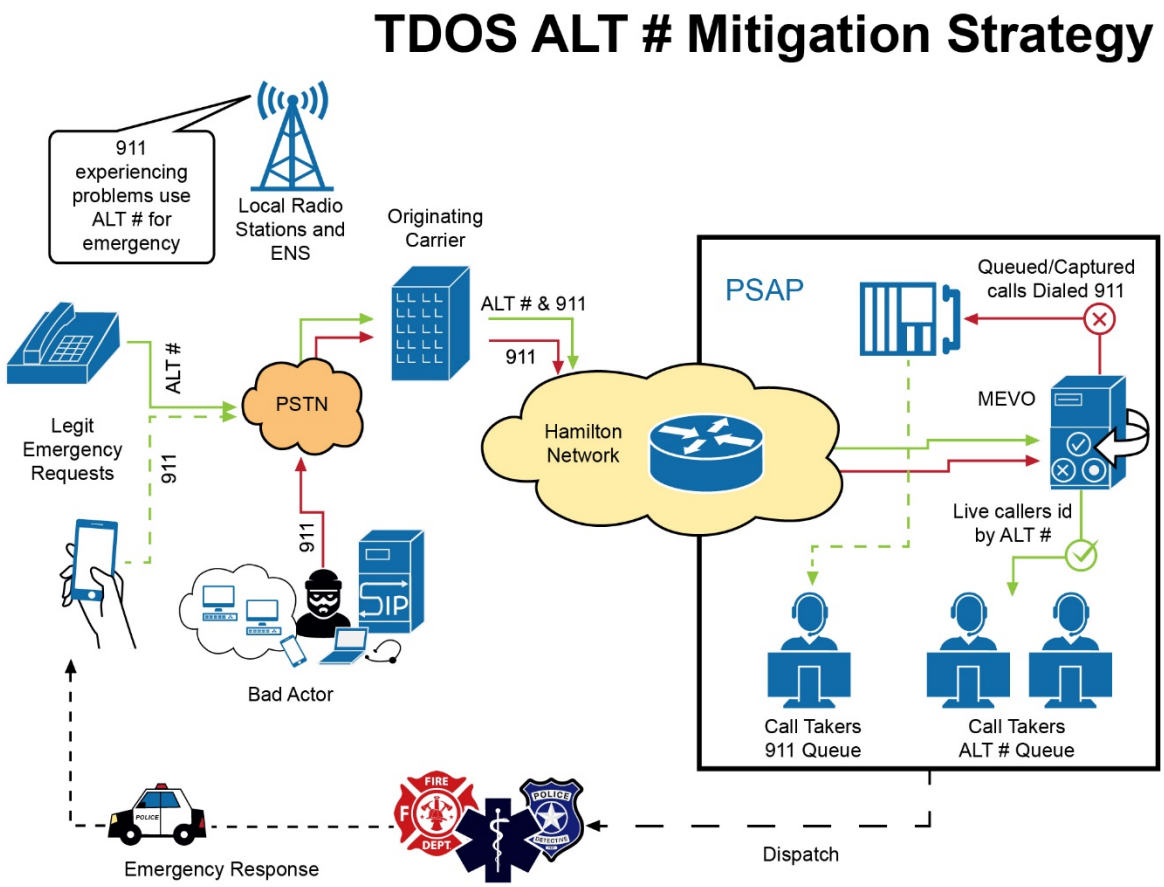
If a common source of the attack can be identified, it will be blacklisted. An Interactive Voice Response (IVR) platform will provide an alternate instruction or customized delivery to the PSAP for emergency services.

If the TDoS/DDoS attack cannot be isolated and live (good) calls cannot be distinguished from the TDoS/DDoS traffic, then other mitigation strategies will be implemented, utilizing methods we have refined over years of experience.

These options vary by the nature of the intrusion, and are not fully disclosed in a public facing document (such as an RFP response). They include implementing a honeypot in the call flow to attempt to gather more call location data, requiring a dual-tone multi-frequency (DTMF) response from the caller, using an alternate number, or utilizing an interactive voice response (IVR) system strategy.

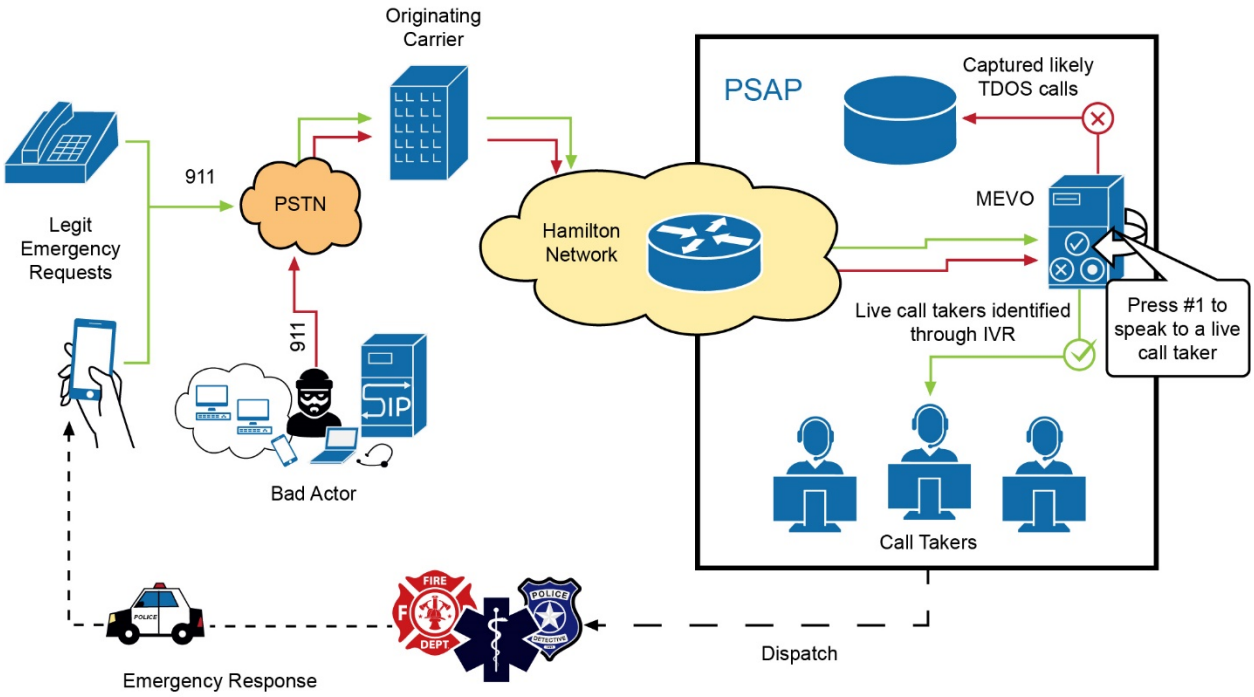
As technology continues to advance, the ATIS SHAKEN / STIR industry standard is expected to become commonly available. Hamilton is developing plans for the implementation of this platform at the time of this response.

Hamilton has fully developed TDoS/DDoS action plans implemented in multiple other NG deployments. These plans will be a component of the proposed solution.



For example, one TDoS Alternate Number Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in a short time span) to listen to an IVR message. This IVR message directs the caller to contact an alternative 10-digit number for their emergency. All other callers are routed to 9- 1-1 normally.

TDOS IVR Mitigation Strategy



The TDoS IVR Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in a short time span) to "press 1" to be connected to 9-1-1. All other callers are routed to 9-1-1 normally.

NOC/SOC 6	**NOC/SOC - Physical Access Monitoring and Management** 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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 6.				

Any additional documentation can be inserted here:

The Hamilton solution provides physical access monitoring and management. The Nebraska Data Center (NDC) and Hamilton's data center, located at its corporate headquarters in Aurora, NE, employ certified safety and security recommended standards, with 24x7x365 environmental monitoring; video monitoring; dual factor access control; fire suppression system; and individually locked equipment cabinets and/or cages.

Hamilton will utilize standard rack access control technology with a combination of keyed locks, smartcard, or RFID fob access. The access control system monitoring will alert our NOC/SOC. In cases where these security methods do not provide an audit

trail, video surveillance and cloud-based alerting and recording will be used. These solutions meet the requirement in a combination of ways, including the CJIS Security Policy, depending on the conditions of the data center.

Hamilton will ensure that physical protection policies and procedures are documented, as well as implemented, to ensure sensitive information, as well as information system software, hardware, and media are physically secure through access control measures. The Hamilton solution ensures for the physical protection of all system resources containing sensitive information.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NOC/SOC 7.				

Any additional documentation can be inserted here:

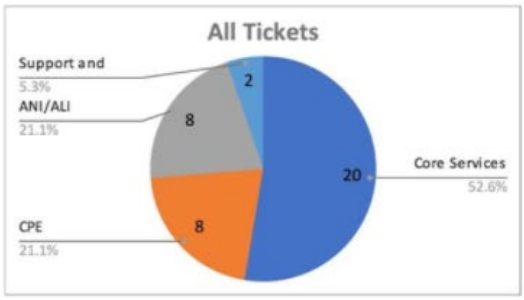
Hamilton's incident management system logs all support requests including those from users and those automatically generated.

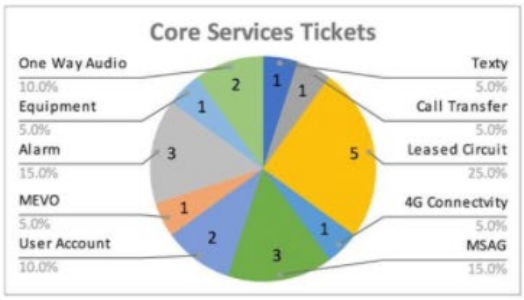
Hamilton provides a 24x7x365 NOC/SOC operation for support documentation and service-related issues. Additionally, Hamilton provides an "In Case of Emergency" number to escalate critical services issues if the NOC/SOC were to be unreachable. An offsite call center, providing backup call support and escalation services, is also available in the event the NOC/SOC were unreachable.

Monthly Reports

In its solution, Hamilton includes monitoring solutions and TeamSupport ticketing. Support requests are manually entered via the web interface and/or auto generated by maintenance tools. Notifications are then distributed to the appropriate distribution list based on requirements.

The example included below is a report detailing tickets opened, pending, resolved, and closed for a time period spanning from 4/12/2020 – 4/18/2020.





From 04/12/2020 to 04/18/2020 → 52.6% Core Services Tickets			
Date	Customer	Issue	Date Closed
04/12/2020	[redacted]	101-121-TALLADEGA-MEVO-04 10.205.121.98 Host Check Timed Out	04/14/2020
04/12/2020	[redacted]	101-025-THVLAL-PR01-gi0/0/1 10.205.215.42 Host Check Timed Out	04/13/2020
04/12/2020	[redacted]	101-073-BESSEMERCITY-NG01-AC-FXS 10.205.173.72 Host Check Timed Out	
04/12/2020	[redacted]	CenturyLink circuit outage	
04/12/2020	[redacted]	101-073-AMVLAL-PR02-4G-VPN 10.205.210.31 / Host Check Timed Out	04/16/2020
04/13/2020	[redacted]	All ECW Positions Down	
04/13/2020	[redacted]	Circuit in alarm	04/14/2020
04/13/2020	[redacted]	Mediacom VPN in alarm	04/13/2020
04/13/2020	[redacted]	101-025-GVHLAL-PR01-gi0/0/1 down	
04/13/2020	[redacted]	101-055-GDSDALCTY-PR02-Comcast-VPN is down	
04/13/2020	[redacted]	ETH100-23415649 is down	04/13/2020
04/13/2020	[redacted]	ALI A down 10.HRXZ.5060419 AT&T ticket EJ 066862	04/14/2020
04/13/2020	[redacted]	MTGALDEX-SBC-A and 101-HVLALASC-SBC-A in alarm.	04/13/2020
04/13/2020	[redacted]	ALI bouncing	04/13/2020
04/13/2020	[redacted]	Position 3 in JVILLE hard drive has failed after a power on cycle of PC	
04/13/2020	[redacted]	Anniston PD door phone cutting out almost not understandable	04/15/2020
04/13/2020	[redacted]	Texty cannot be reached.	04/13/2020
04/13/2020	[redacted]	Site CPE Alarms	04/15/2020
04/13/2020	[redacted]	MEVO Changes	04/15/2020
04/13/2020	[redacted]	ALI1 not pingable	
04/13/2020	[redacted]	911 calls with no ALI/ANI	04/13/2020
04/13/2020	[redacted]	IRR at station 3 will not replay	04/13/2020
04/14/2020	[redacted]	Pos 1 time is off 2 hours	04/14/2020
04/14/2020	[redacted]	AL911.net - Contact Form Submission	04/14/2020
04/14/2020	[redacted]	Road update	
04/15/2020	[redacted]	911 call hangs up it shows abandoned and then another call shows up with the sa	04/15/2020
04/15/2020	[redacted]	Reestablish User: Carly Bradley	04/16/2020
04/16/2020	[redacted]	Cannot xfer 911 calls to SO on POS1 and POS2	04/16/2020
04/16/2020	[redacted]	ALI B link bouncing.	
04/16/2020	[redacted]	New street	04/16/2020
04/16/2020	[redacted]	ALI link A down	
04/16/2020	[redacted]	Position 5 Genovation not working	
04/17/2020	[redacted]	ANI failures	
04/17/2020	[redacted]	Needs report for agency	
04/17/2020	[redacted]	Insert into MSAG : Walnut Hill Dr and Walnut Hill Ln	04/17/2020
04/17/2020	[redacted]	NRF/Ghost calls coming in on landline trunk 5, their telco is CL	04/19/2020
04/18/2020	[redacted]	No internet	04/18/2020
04/18/2020	[redacted]	Stuck call	

Service Impact Levels

The following matrix outlines Service Impact Levels including notification times and response times:

SERVICE LEVEL IMPACT	INCIDENT TYPE	COMMUNICATION METHOD FROM SERVICE PROVIDER TO CUSTOMER (all listed methods)	TICKET INITIATION	UPDATE FREQUENCY (e-mail)	RESTORATION NO LATER THAN
Tier 1 - Critical Full loss of critical functionality	Trunk outages, Alternative Routing Activation, All calls misrouting, No ANI/ALI, Loss of service, FCC reportable incidents, PSAP unable to perform core functions, Transfer failures (all calls), Circuit outage, Ransomware or Malware attack	Phone Text Email	≤15 minutes	≤1 hour	≤4 hours
Tier 2 - Major Partial loss of critical functionality	Intermittent misroutes, Intermittent transfer failures, Intermittent ALI issues, no/incorrect data, WAN links bouncing intermittently, Inability of PSAP to support 9-1-1 calls due to equipment failures	Phone Text Email	≤30 minutes	≤2 hours	≤8 hours
Tier 3 - Minor Does not have serious impact	Occasional calls Misrouting, occasional transfers to other PSAPs failures, PSAP equipment issues that do not impact call taker response	Phone Email	≤1 hour	≤24 hours	≤7 calendar days
Tier 4 - Maintenance Does not have serious impact or informational	Non-Critical and informational request Maintenance Activities	Email	≤2 hours	≤weekly	≤30 calendar days

Tickets submitted as non-emergent, or not immediately assigned a severity level, along with any tickets that are left idle, will automatically cause notifications to be sent to NOC/SOC personnel.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 8.				

Any additional documentation can be inserted here:

Hamilton's proposed solution includes a change management system with the ability to provide the Commission's program manager and designated Regional Call Host (RCH) representatives with the ability to review proposed change requests and the client approval process. On a monthly basis, Hamilton will provide reports detailing change tickets opened, pending, resolved, and closed.

Hamilton's solution for reporting and data collection, 911 Logix, will provide enterprise-wide reporting specific to PSAPs and is customizable, providing an efficient and transparent way to monitor, report, and analyze data. 911 Logix will provide the means for the Commission to request changes and receive updates on progress.

Nebraska's customized web portal, NE911.net, will provide a real-time view of the network, including the drill-down capability to a specific device. This portal will allow the Nebraska NG 9-1-1 network and PSAPs to cooperatively view, track, and manage the solution.

NOC/SOC 9	**NOC/SOC - Change Management System** **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: Hamilton complies with requirement NOC/SOC 9.				

Any additional documentation can be inserted here:

As mentioned above in Requirement NOC/SOC 8, Hamilton's solution for reporting and data collection, 911 Logix, will provide enterprise-wide reporting specific to PSAPs and is customizable, providing an efficient and transparent way to monitor, report, and analyze data.

In addition, Hamilton will provide the state with access to the NE911.net web-based portal. The portal will provide the Commission with a real-time view of the network, including the drill-down capability to a specific device. This portal will allow the Nebraska NG 9-1-1 network and PSAPs to cooperatively view, track, and manage the solution.

NOC/SOC 10	**NOC/SOC – Change Management System** **Change Testing and Training Environment** A non-production ESInet replica / 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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 10.				

Any additional documentation can be inserted here:

Hamilton has included an in-market lab environment as part of the proposed solution. This system can be used for non-production and pseudo production testing of interoperability between vendors and local authorities as well as for training purposes.

Additionally, we maintain a quality assurance (QA) lab using the current release of in-production hardware and software for testing software or hardware changes. Additionally, if needed, we can provide a conformance lab for state office stakeholders to verify equipment and failover scenarios.

Through a well-defined system testing infrastructure, Hamilton provides trusted and established innovative services. To ensure operational standards, the system test plan reflects flexible processing, defined benchmarks, case-by-case assessment, and the ability to meet the unique requirements of the state. The main goals of this process include meeting the Commission's operational objectives, maintaining cost-efficiency, and delivering expected quality.

The Hamilton testing environment and subsequent data emulates the live operational environment as much as possible. Such infrastructure is conducive for adequate simulation and will be repeatable and quantifiable while providing measurable activity. Testing will be divided into distinct phases, each with clearly defined objectives and goals. Phases will follow an established workflow of:

- Entrance and Exit Criteria
- Acceptance Testing
- Test Cases and Scenarios
- Fail Over
- Reporting and Data Sharing

The testing activities will be built upon previous stages, diminishing undue redundancy and/or duplication of effort. Hamilton ensures a system testing plan that executes common, consistent procedures for all necessary staff, testing activities and resulting performance. The state may inspect test equipment and/or make additional request at any point if desired.

A sample of a comprehensive Sample Test Plan (PROPRIETARY CONFIDENTIAL) is included as Appendix 8. This test plan is from another jurisdiction, which will be refined to the Nebraska NG 9-1-1 ESInet.

NOC/SOC 11	**NOC/SOC – Change Management System** **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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 11.				

Any additional documentation can be inserted here:

Change Management Process & ITIL Standard

Hamilton's solution includes an established change management process that complies with the Information Technology Infrastructure Library (ITIL) for continuous service improvement as part of its organizational culture. This process follows the five ITIL stages of continuous service improvement and ensures that standardized methods and procedures are used. For efficient and prompt handling of changes, Hamilton's approach is to minimize the negative impact of improperly defined and managed project changes, resulting in improved day-to-day operations of the project. Change management is all about understanding and managing of risk and Hamilton has established strategies and capabilities to ensure that new changes can be deployed without any disruption or downtime.

Change Control Process for Planned Vs. Unplanned Change Management

Unplanned, or emergency changes, may be warranted at times and Hamilton's solution includes documented change management processes for both scheduled and emergency changes. These processes are described below:

I. Planned Change Management

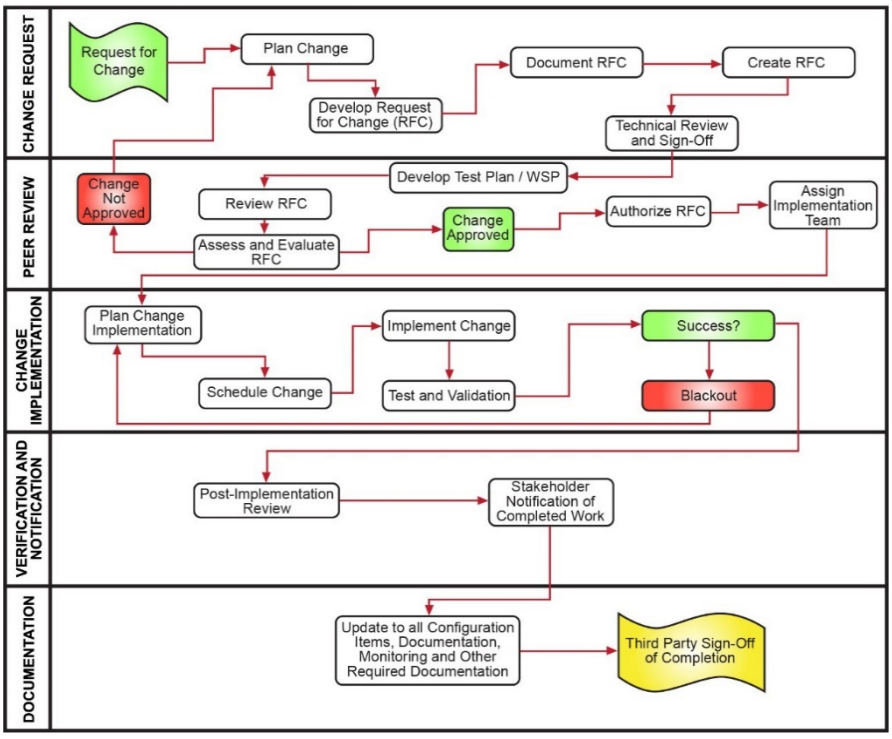
Effective change management is of vital importance to emergency communications systems. If not managed correctly, changes introduce unnecessary risk. We manage this risk by following processes to help us analyze and plan the change, then implement the change in a controlled and considered manner. The complexity and rigor of the change management process depends on the magnitude and impact of the change. During the planning phase of the project, a Change Register Report (CRR) will be created specifically for the Nebraska NG 9-1-1 project and submitted for approval by the designated Nebraska NG 9-1-1 Project Manager.

All system changes require technicians to create a Change Management Process (CMP). The primary goal of the CMP is to require technical staff to create a plan, get technical sign off, document work, verify results, advise stakeholders of planned work and notify stakeholders upon completion.

After action reports (AAR) are a component of the CMP and are generated following all system changes, whether there was a negative impact to system performance or not. This allows for documentation of all pertinent information generated during system change processes.

All CMPs, including AARs, are made available to the customer. Please see the change management process in the figure below.

CHANGE MANAGEMENT PROCESS



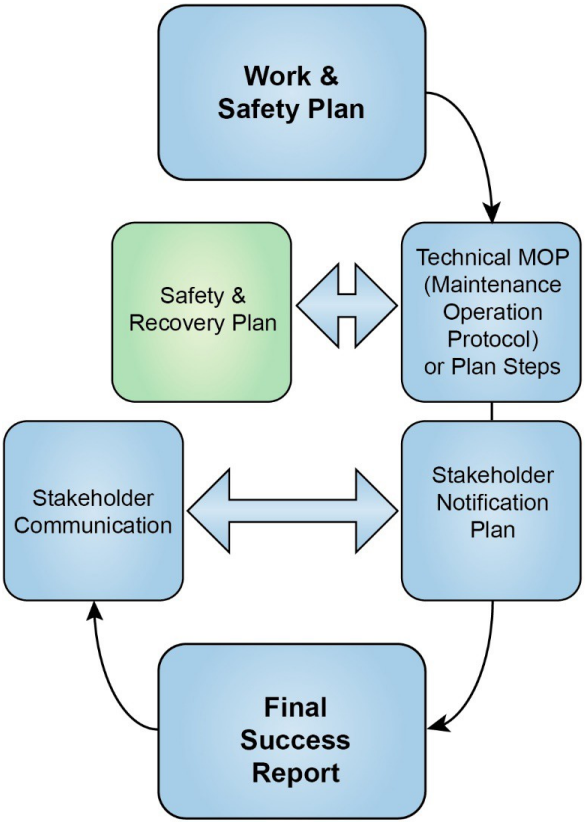
II. Unplanned Change Management

Unplanned change events are typically emergency maintenance events. The same change control and maintenance notification processes utilized during planned events are also required as part of an unplanned event.

Notification to customers and other parties is required before any unplanned maintenance event. Notifications provide a summation of the work to be performed, along with an advisory as to the likeliness of the event causing an interruption in normal operations.

Work processes during an unplanned event are also required to follow similar procedures to a planned event. For example, a Maintenance Operation and Protocol (MOP) document must be created and approved by appropriate management prior to the completion of work.

The goal during an unplanned event is to ensure as much planning and communication is completed to ensure seamless call delivery.



Change Management Notification Process

As mentioned directly above, Hamilton's MOP document is an established step within its change management process. In conjunction with its 9-1-1 system stakeholders, Hamilton has created industry-leading maintenance procedures and work guidelines. The process for planning any scheduled maintenance activities is as follows and is illustrated in the diagram below. The overall work and safety plan (WSP) was created to provide notification and transparency to 9-1-1 system stakeholders. The WSP focuses on documenting a primary plan, creating a backup plan, peer review, results verification, and stakeholder identification. If maintenance work is needed, Hamilton creates a comprehensive document describing what work needs to be completed and a step-by-step guide on the work that will be completed.

Once the plan has been created, notification is provided to all stakeholders. Additionally, WSP work is scheduled in a pre-defined maintenance window with prior notification required to designated points of contact.

Within the MOP, technical work is described and expected maintenance results are defined. in the. Once maintenance has been completed, a final success report is issued, and all stakeholders listed within the MOP are notified with results.

Also, within the MOP document, is a safety and recovery plan if maintenance work does not go as anticipated. If this were to occur, Hamilton will return to the service restoration plan contained in the WSP. We have found this process to be extremely successful in creating an environment of consistent quality results.

The maintenance provided by Hamilton includes all preventative scheduled maintenance and Hamilton will provide all maintenance services to ensure the service remains in good operating condition.

Fault, Configuration, Accounting, Performance, & Security (FCAPS) Procedures

Hamilton's network operations center/security operations center (NOC/SOC) provides comprehensive system administration capabilities that are customized based on the operational needs of Nebraska's NG 9-1-1 system and stakeholders. As detailed above, Hamilton has ensured that proper change management processes are in place and properly followed to improve service, manage change, and minimize downtime. Hamilton's robust change management process follows the Fault, Configuration, Accounting, Performance, and Security (FCAPS) model which defines the functions and capabilities needed for comprehensive operations management. Further, FCAPS identifies the following capabilities as necessary for comprehensive network management:

- Fault Management - Fault management is implemented and maintained to ensure no Single Point of Failure (SPF) exists. This includes, but is not limited to, all technical, environmental and logical aspects of the solution. Potential future problems are identified, and steps are taken to prevent them from occurring or recurring.
- Configuration - Network operation is monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems

and programs, are coordinated. Inventory of equipment and programs is kept and updated regularly.

- Accounting - Distribution of resources are done optimally among network users. This makes the most effective use of the systems available, minimizing the cost of operation.
- Performance - While managing the overall performance of the network, throughput is maximized, network bottlenecks are avoided, and potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement.
- Security - The network is protected against hackers, unauthorized users, and physical or electronic sabotage. The confidentiality of user information is maintained where necessary or warranted. Security systems also allow network administrators to control what each individual authorized user can (and cannot) do with the system.

ITIL & FCAPS Processes

As documented above, Hamilton's proposed solution supports and complies with the requirements for the ITIL and FCAPS processes. Compliance with these processes is of the utmost importance to Hamilton and is absolutely necessary in order to deliver superior results. Incorporating these processes into our change management system, and our larger NOC/SOC operation, ensures Nebraska will receive the full benefit of the implemented IP-based NG 9-1-1 solution.

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).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 12.				

Any additional documentation can be inserted here:

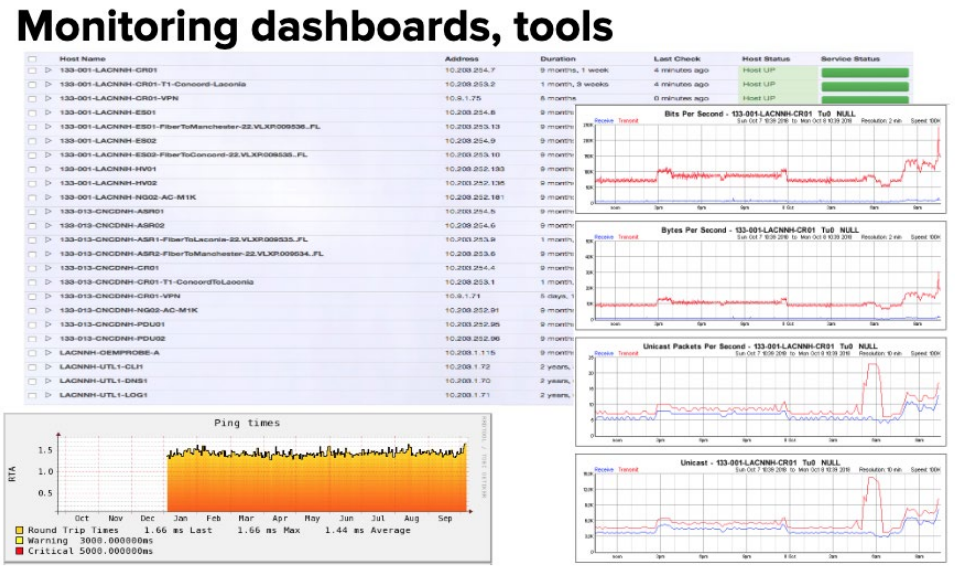
Hamilton has the appropriate toolset to provide Regional Call Host (RCH) network management information software (NMIS), network analytics, and visualizations. Hamilton's NMIS captures, analyzes, and reports on the network's health based on the Simple Network Management Protocol (SNMP) traffic it receives. In addition to providing all required reports, our submission includes numerous dashboards to provide metrics at the PSAP, Regional and Statewide level.

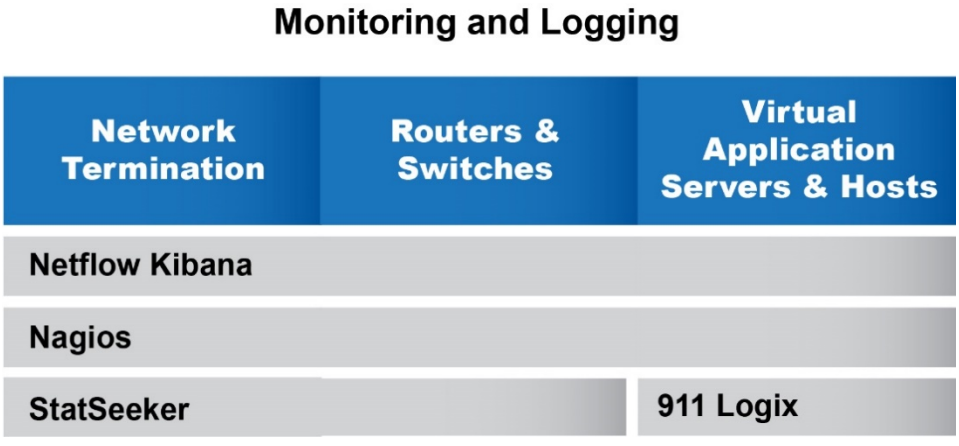
Hamilton uses several platforms for alarms and monitoring of systems (depending on function and system). These network tools include:

- NAGIOS
- Statseeker
- 911 Logix
- Logging Subsystem
- Netflow/Kibana
- Forticloud/Fortiview

Dashboards include:

- Providing comprehensive visibility for all systems listed above
- Notifications
- Visual
- Text/ email/ PSNA display





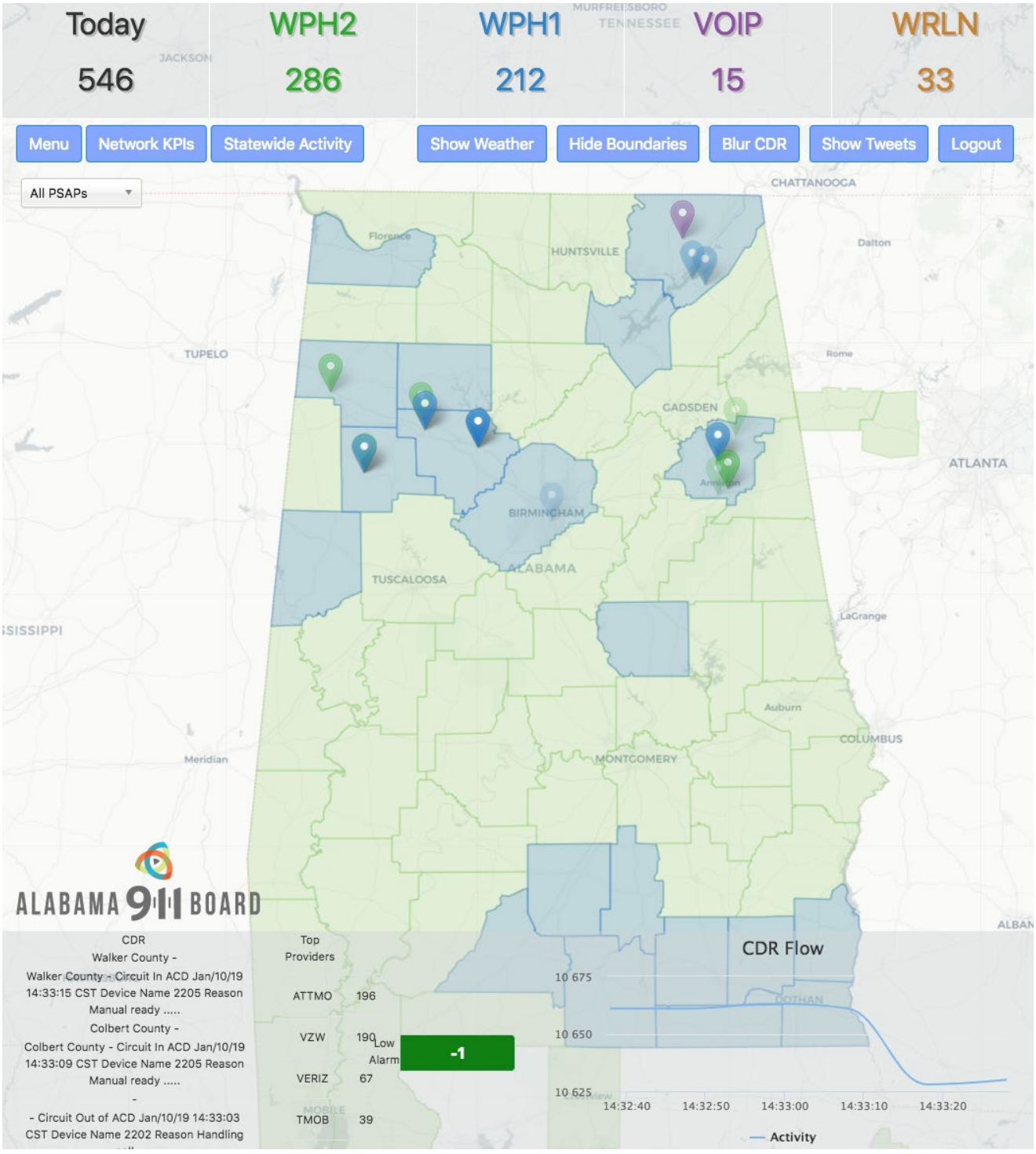
The dashboards and reports are accessed via a centralized dashboard. The dashboard and associated reports are provided as a suite of products with the tradename “911 Logix.” 911 Logix is accessed via a secure dual authentication method provided by “Duo”. Once securely logged on, the user can access data and reports via any desktop or mobile device.

Additionally, new reports are added periodically when users determine that an additional report is required. Our model is predicated on the fact that when a user identifies the necessity for a new report, this report will have utility for other users as well. Therefore, we produce the report and update the 911 Logix system so that all users have access to the report. These new reports are provided as part of the service. In summary, if the data is available and the user requests a report that can be used by multiple PSAPs, then Hamilton will work with Nebraska to produce a new report and make it available to all users.

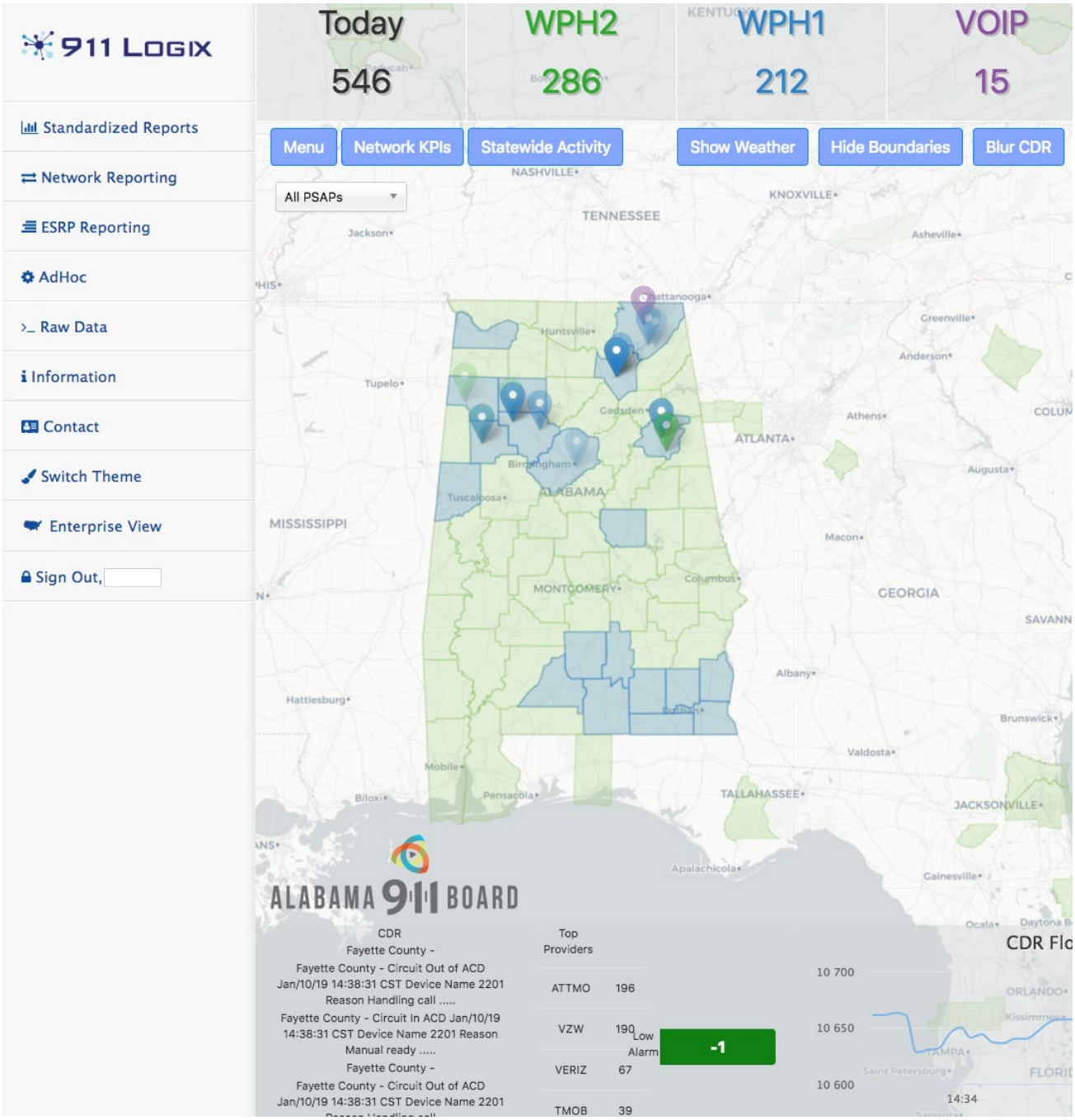
911 Logix and all dashboards and visualizations are set up with a hierarchical method so that access to data is available by permissions. Hamilton will work with Nebraska to determine initial access credentials and the requirements for password formats and security levels. Once installed, permissions and logon credentials can be managed as part of the service.

Hamilton will provide standard reports, NMIS tools, and performance metrics to be made available to each Regional Call Host (RCH) and the state of Nebraska monthly or upon request.

Some examples of reports include:

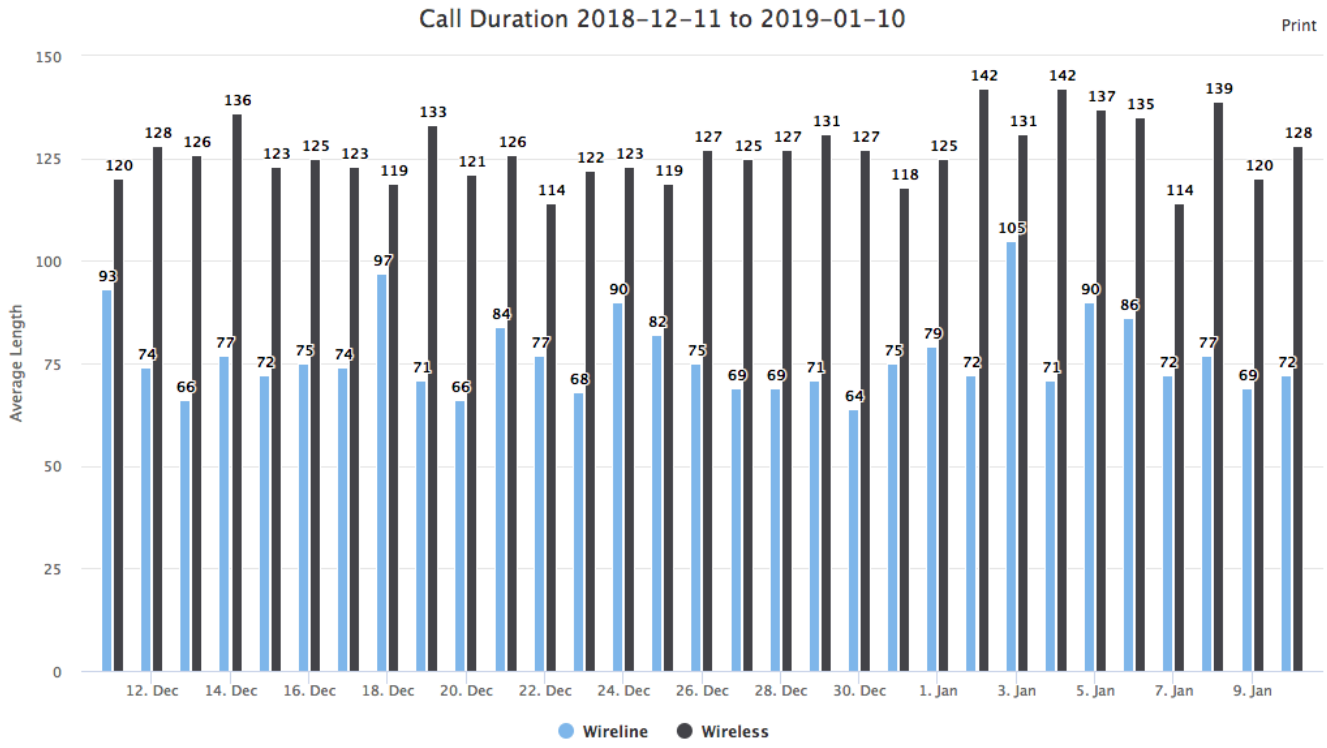


The example above shows the PSAP or Regional interface for tracking 9-1-1 Call Activity and accessing reports.



The example above shows the report interface along the left side of the dashboard displayed when the "menu" button is selected.

Menu | Change Chart Type | Select Start | Select End | All PSAPs | Print Page



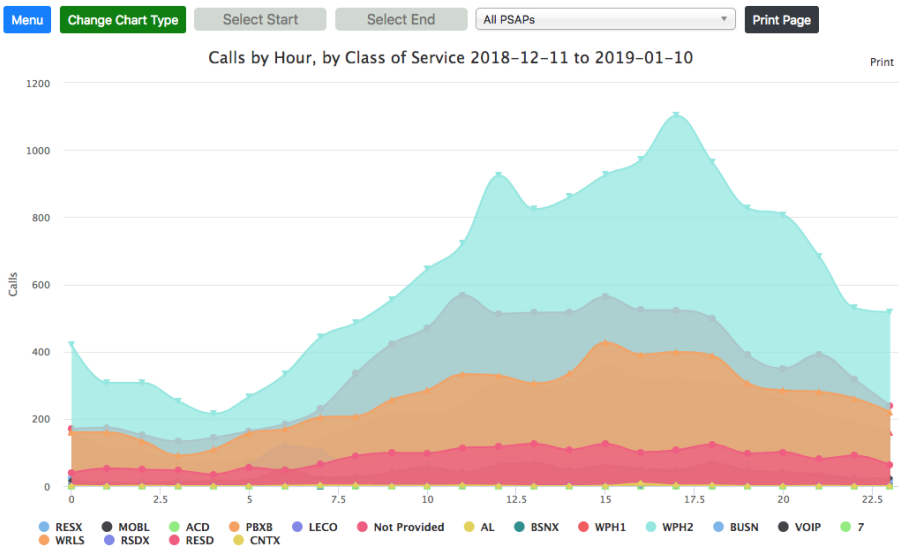
Copy CSV PDF

Search:

Average	76.84	126.65

Date	Wireline	Wireless
2018-12-11	93	120
2018-12-12	74	128
2018-12-13	66	126
2018-12-14	77	136
2018-12-15	72	123
2018-12-16	75	125
2018-12-17	74	123
2018-12-18	97	119
2018-12-19	71	133
2018-12-20	66	121

Call Volumes by Call Type



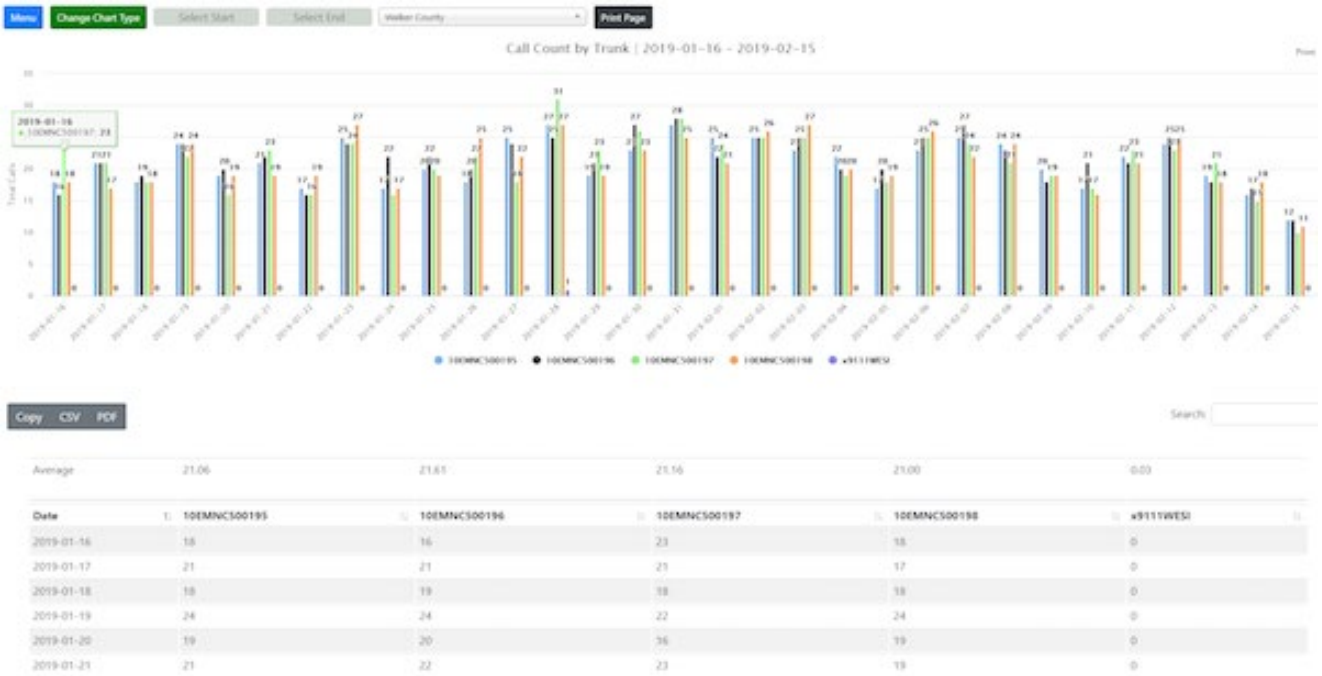
Copy CSV PDF

Search:

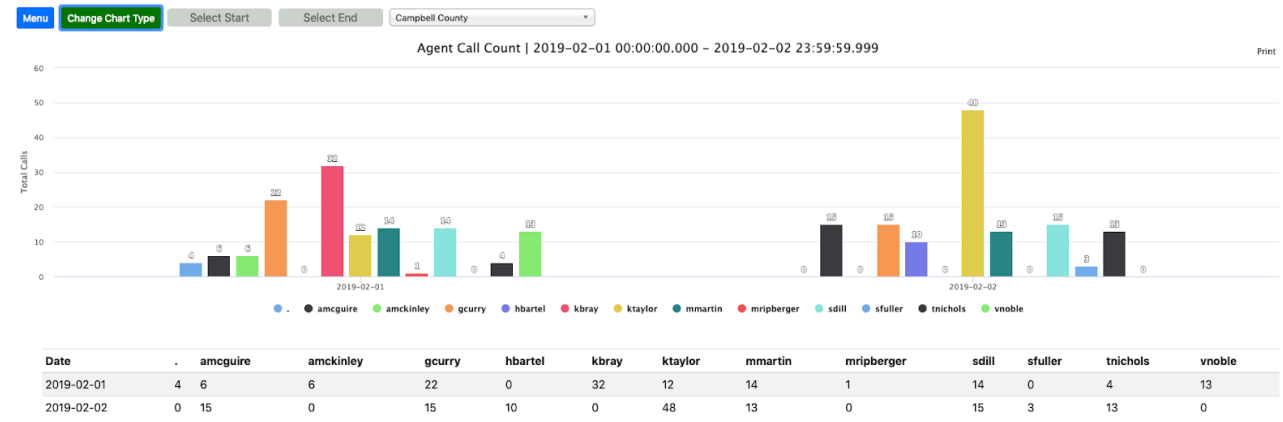
Average	28.35	23.81	22.23	17.97	17.45	23.84	28.87	35.39	40.35	48.52	54.32	62.13	68.32
Totals	879 (2.5%)	738 (2.1%)	689 (2.0%)	557 (1.6%)	541 (1.5%)	739 (2.1%)	895 (2.5%)	1097 (3.1%)	1251 (3.5%)	1504 (4.3%)	1684 (4.8%)	1926 (5.5%)	2118 (6.0%)

CallDate	0	1	2	3	4	5	6	7	8	9	10	11	12
2018-12-11	24	14	9	22	15	32	25	48	49	53	62	62	60
2018-12-12	20	15	13	13	11	24	37	30	40	38	48	56	43
2018-12-13	18	22	15	20	14	14	35	50	45	56	62	54	69
2018-12-14	22	14	17	13	11	14	26	47	54	41	30	26	59
2018-12-15	29	25	24	8	43	33	24	40	57	43	54	56	92

Call Count by Trunk



Event by Incoming IP Address



Date	.	amcguire	amckinley	gcurry	hbartel	kbray	ktaylor	mmartin	mripberger	sdill	sfuller	tnichols	vnoble
2019-02-01	4	6	6	22	0	32	12	14	1	14	0	4	13
2019-02-02	0	15	0	15	10	0	48	13	0	15	3	13	0

Agent Report, By Region or PSAP

NOC/SOC 13	**NOC/SOC – Network Management System** **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: Hamilton complies with requirement NOC/SOC 13.				

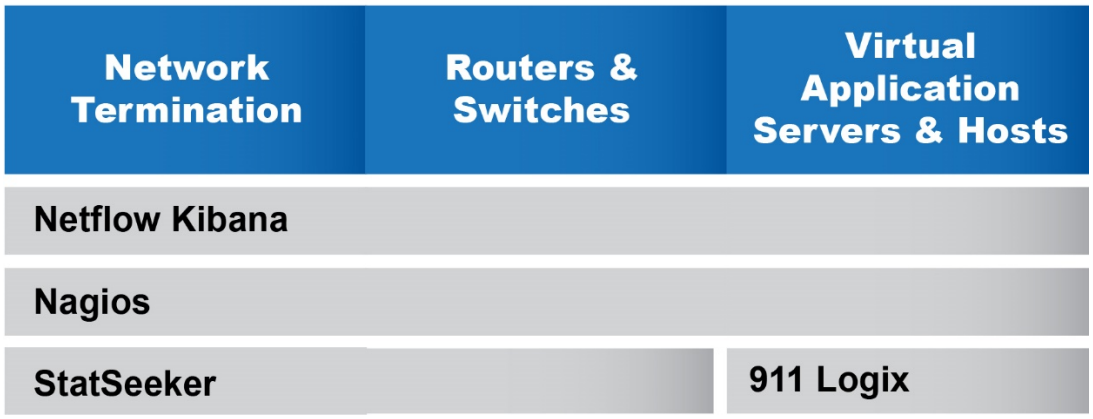
Any additional documentation can be inserted here:

Hamilton's proposed solution interworks with all the various elements and services of the Hamilton NG 9-1-1 system and network elements. To accomplish this, Hamilton uses several platforms for alarms and monitoring of systems (depending on function and system). These network tools include:

- NAGIOS

- Statseeker
- 911 Logix
- Logging Subsystem
- Netflow/Kibana
- Forticloud/Fortiview

Monitoring and Logging

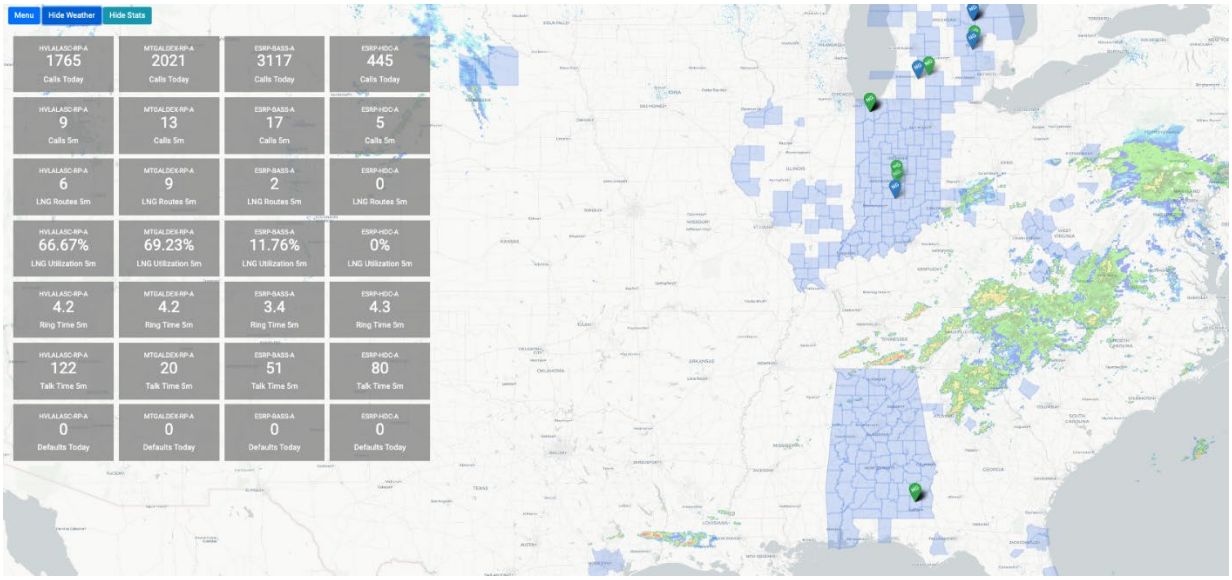


NOC/ SOC 14	**NOC/SOC - Network Event Logging** **System and Network Event Logging and Reporting** The network management system shall capture real-time and historical tracking of network and system events, as well as event resolution of the IP network and attached systems. This is for logging errors 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 as part of NGCS Option B requirement NGCS 13 Event Logging. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 14.				

Any additional documentation can be inserted here:

Hamilton's proposed solution includes a network management system that captures real-time and historical tracking of network and system events, as well as event resolution of the IP network and attached systems. Some events include hardware (e.g. power, processor, interface cards, and ports), software (e.g. operating system errors, database errors, application errors, and failures), and network (e.g. Quality of Service (QoS), Mean Opinion Score (MOS), jitter, latency, and packet loss). Hamilton collects event logs from the various network elements (NE) and functional elements (FE) in the NGCS core, as well as network events from the tools that are used to surveille and monitor the network. This enables us to log, display, and report on errors. The proposed solution will alert through dashboard visualizations and notification methods.

The example below provides for just one view of a visualization and key performance indicators (KPI) that can be presented based on logs collected at the application and network level.



The legacy network gateway (LNG) FE of Hamilton's proposed solution is capable of logging all significant events and 9-1-1 calls received and processed. However, the events recorded and detailed within this section are not related to the event logging of 9-1-1 requests for service completed by the LNG FE. Logging by the LNG FE is further detailed in NGCS Option C requirement NGCS 13 Event Logging.

NOC/SOC 15	**NOC/SOC - Network Event Logging 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 requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NOC/SOC 15.				

Any additional documentation can be inserted here:

Hamilton's network performance data from various network operations center/security operations center (NOC/SOC) system management tools (e.g. Statseeker, Nagios, etc.) and functional elements (FE) is consolidated within Hamilton's 911 Logix platform to provide the NOC/SOC with a holistic view of the events taking place within the network. 911 Logix gives the NOC/SOC access to consolidated dashboard representing network activity, as well as the ability to query any pertinent piece of data to create a 'ladder' type diagram of the call flow, showing how the call moved through the network and each FE.

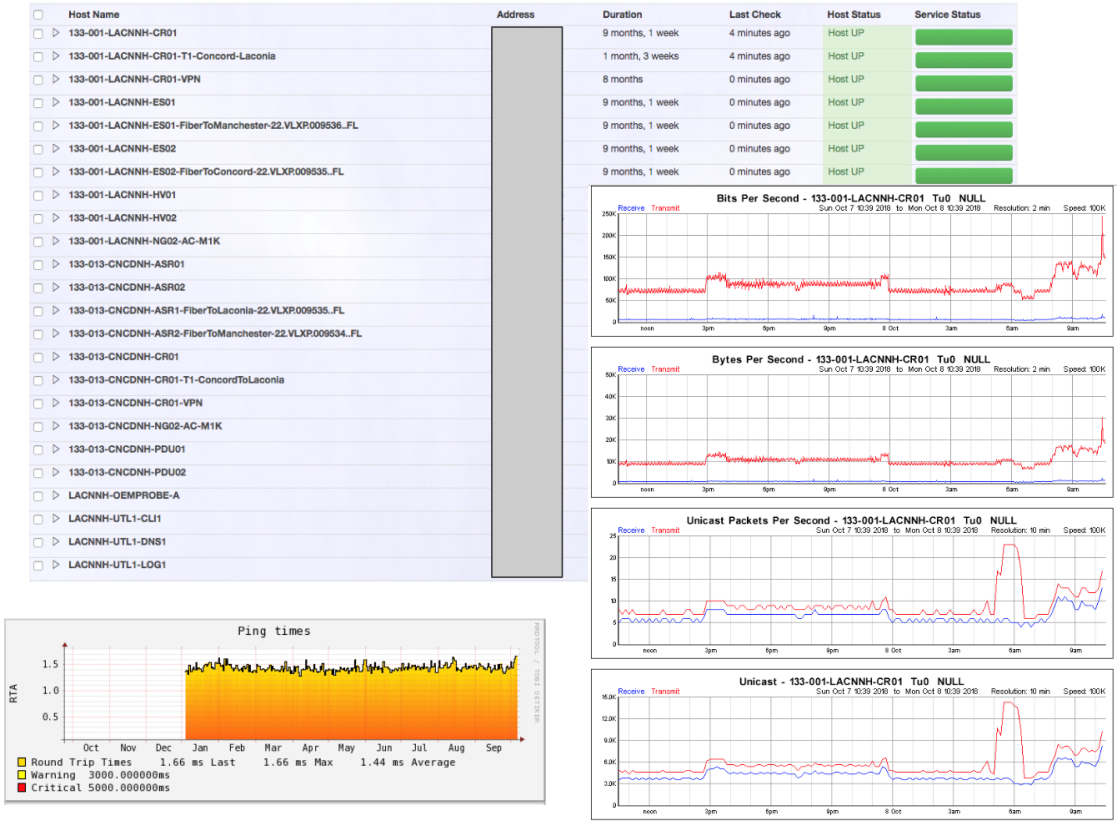
Historical information, including logs from all FEs and monitoring platforms, will be maintained for the term of the contract as required. Copies of data will be provided to the Commission on a confidential basis upon request.

NOC/SOC 16	**NOC/SOC - Network Event Logging 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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NOC/SOC 16.				

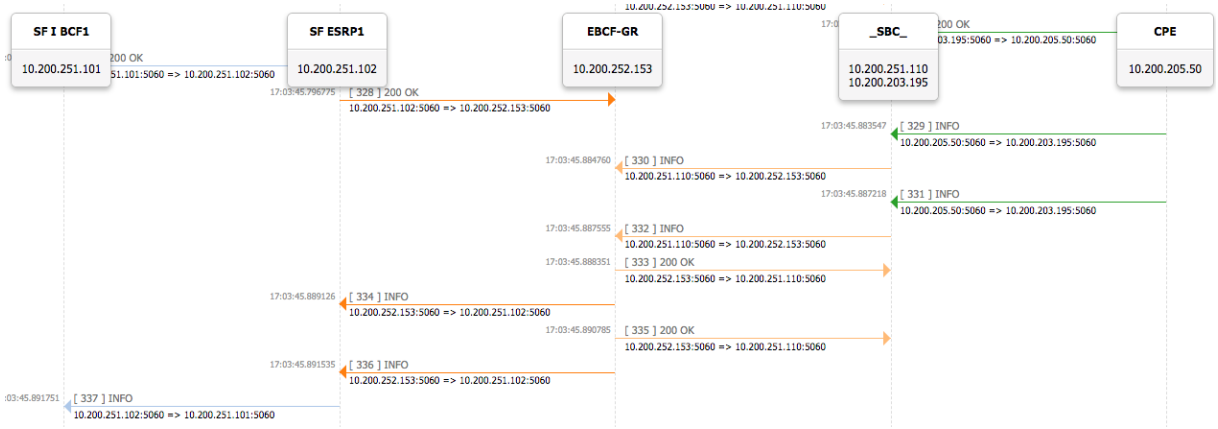
Any additional documentation can be inserted here:

Hamilton will provide a dedicated 24x7x365 network operations center/security operations center (NOC/SOC), specializing in 9-1-1 service management, which will serve as a single point of contact for all PSAPs, interconnecting parties, and designated Nebraska NG 9-1-1 staff.

A full portfolio of monitoring tools and active alarming are employed to identify potential problems before they occur. The NOC/SOC utilizes monitoring systems to log and alarm all facets of 9-1-1 services in near real time. This includes bandwidth usage, memory usage, CPU usage, and services availability. This includes all devices in the core and edge.



The monitoring solution provides audio and visual alarming to the NOC/SOC. Alarms originating from critical applications and services notify appropriate engineers immediately and directly of possible problems. Additionally, packet level captures are collected within the core to provide the ability to recreate the session initiation protocol (SIP) call flow in a ladder diagram.

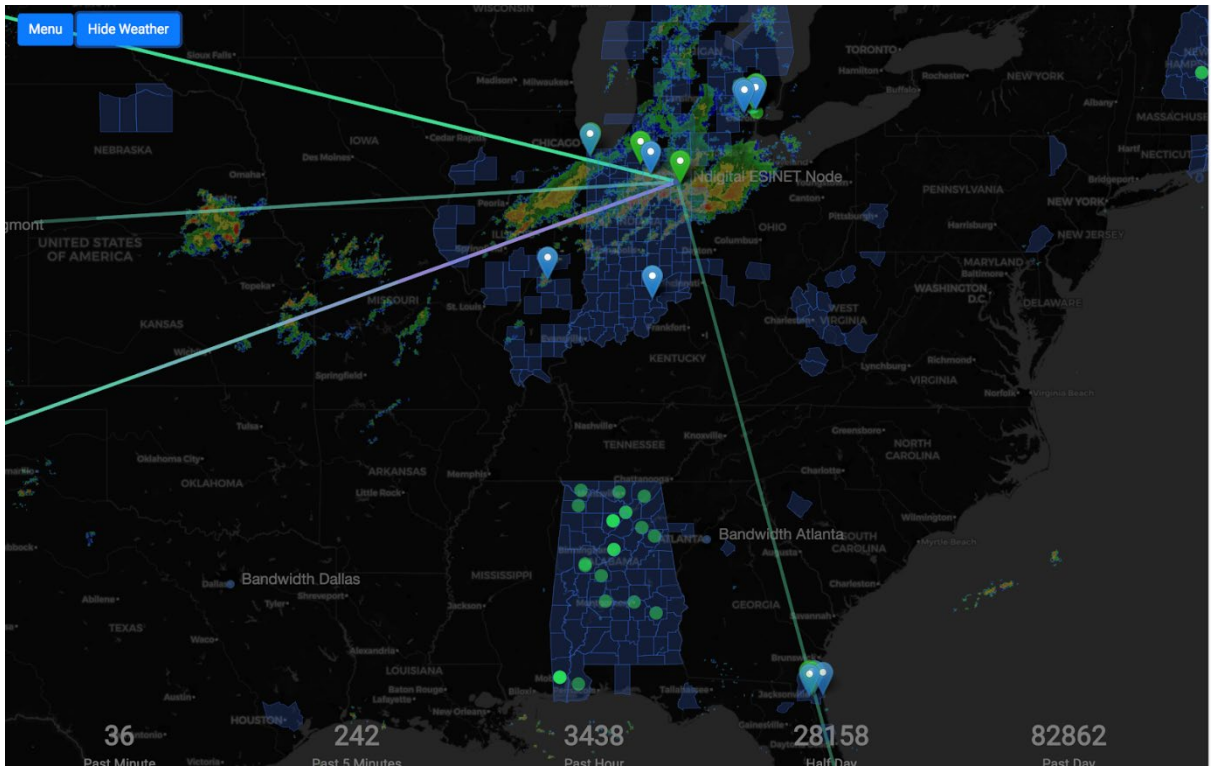


Tickets can be submitted via any of three methods. These include contacting the NOC/SOC through the toll-free phone number, email, or by utilizing the designated online trouble ticketing system.

NOC/SOC personnel will ask a series of questions to help identify the severity of the problem, escalating to appropriate engineers as needed. Most general support issues can be resolved directly by NOC/SOC personnel.

Trouble tickets are created for every request to the NOC/SOC. Designated contacts are notified when a ticket is opened and will receive email notifications as the ticket is updated and resolved. Tickets of a more severe nature will prompt an immediate outbound phone call from the NOC/SOC to the designated recipients.

The solution also provides dashboards with comprehensive 9-1-1 call data with threshold alarming for next generation core services (NGCS) elements. These dashboards allow stakeholders to proactively monitor systems, statistics and visualizations in near real time.



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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 17.				

Any additional documentation can be inserted here:

Communication with Technical Personnel

Hamilton provides a 24x7x365 network operations center/security operations center (NOC/SOC) operation for support documentation and service-related issues. The NOC/SOC is also responsible for communicating with external personnel, such as subcontractor personnel, the Commission, and participating PSAPs and serves as a single point of contact for these parties. Hamilton utilizes a variety of communications methods to ensure that the correct technical personnel are notified and to maintain contact with external personal. These methods of communication include typical telecom systems, email, or by utilizing the trouble ticketing system. Hamilton also provides an “In Case of Emergency” number to escalate

critical services issues if the NOC/SOC were to be unreachable. Additionally, Hamilton has an offsite call center that provides backup call support and escalation services.

Service-Related Issues

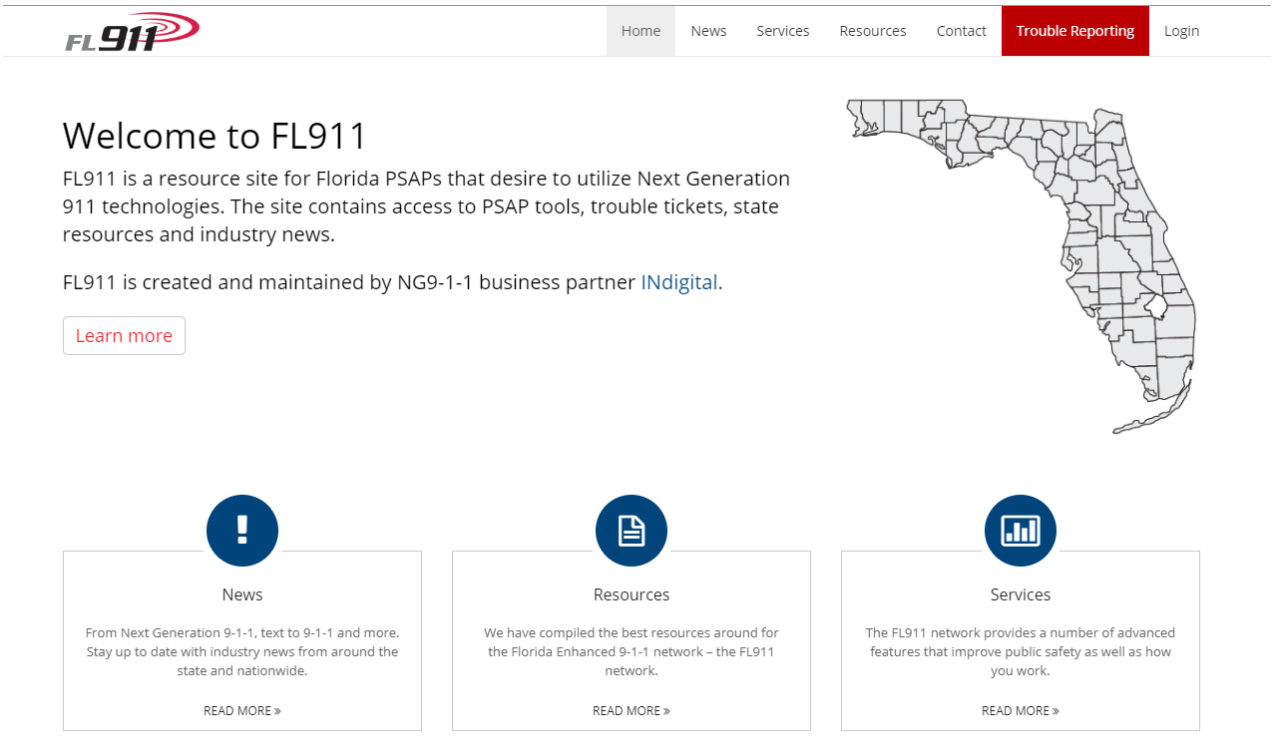
The level of assistance required to resolve service-related issues greatly depends on the severity of the issue. During an outage scenario, the NOC/SOC will immediately escalate to appropriate staff. If service issues could compromise service level agreements (SLA), staff will escalate to senior management via mass notification application. A pre-arranged outage voice bridge will be established to coordinate restoration efforts.

Senior management staff has identified a Media Contact, specified in SLA 21, to execute the pre-defined media communications and stakeholder notification plan.

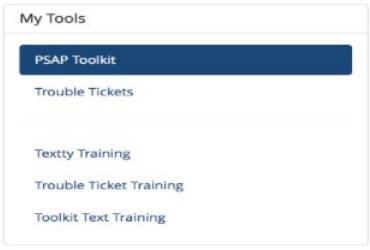
In the unlikely event of malicious attack, the response team is expanded to the Executive, CTO, and Security Officer levels, who would be involved in developing and deploying a solution to resolve the issue.

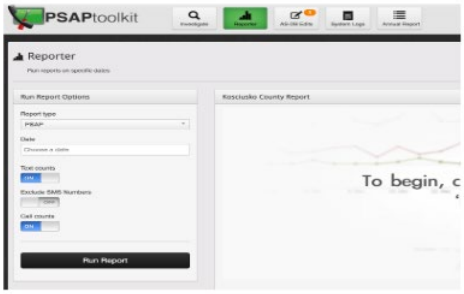
Hamilton uses several alternative ways of communicating with staff. These methods of communication include typical telecom systems, as well as alarms and alerts through email, online messaging systems, and direct messaging software applications to provide internal mass notification.

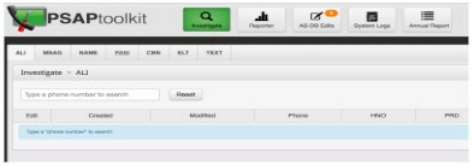
Examples of customer-facing portals are provided in the images below. If awarded the contract, Hamilton would deploy NE911.net as a portal, providing the state of Nebraska with access to 911 Logix, training and configuration documents, etc.



Illinois Trouble Ticket & Toolkit







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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 18.				

Any additional documentation can be inserted here:

The Hamilton network operations center/security operations center (NOC/SOC) informs the Commission and affected PSAPs, or their designees, of problems with the network, scheduled service and maintenance outages, and upgrades. Hamilton's notifications are customized to meet FCC regulations and the operating needs of the state, county, and federal stakeholders. As a 9-1-1 Service Provider in other states, we are accustomed to providing maintenance notices to all stakeholders, including impacted PSAPs and their designees, if there are problems with the network, schedule service and maintenance outages, and upgrades.

Additionally, notifications are provided when service impairments are identified within our network, or those of originating service providers (OSP) connected to the ESInet.

The NOC/SOC notifies stakeholders via voice and electronic notification. Notifications for scheduled maintenance activities or outages will be made no less than ten (10) business days in advance, except for emergency situations. In emergency situations, notification will be provided immediately. In addition, tickets related to the services delivered to subcontracts will be forwarded immediately. In critical outage scenarios, top level management is involved to provide stakeholder communication and restoration efforts. In the unlikely event of a longer duration outage, a conference bridge will be deployed for stakeholder organization and communication on a real time basis.

In the event of an outage and/or impairment in service, Hamilton will notify the Commission and affected PSAPs within 15 minutes of discovering an event and/or outage that may impact 9-1-1 services. Available information useful in mitigating the effects of the event and/or outage will be provided, in addition to name, telephone number, ticket/reference number,

and email address at which the service provider can be reached. Hamilton accepts responsibility for collecting data and troubleshooting and reporting on behalf of its suppliers.

Additionally, notifications are provided when service impairments are identified within our network, or those of originating service providers (OSP) connected to the ESInet.

The next generation core services (NGCS) nodes, functional, and network elements, as well as the services they provide, are self-healing from the call taker perspective. On all known failure states, the redundant and diverse systems will be configured to automatically maintain continuity of service. This is accomplished by having all functional elements in the call chain assigned multiple delivery destinations, A and B geographic redundancy, and by utilizing Hamilton's MEVO(+) disaster recovery platform. Additionally, Hamilton utilizes self-healing routing protocols within the ESInet to re-route IP traffic in the event of a circuit failure.

The Hamilton NOC/SOC serves as the central role as a source of status and additional information and uses a notification and reporting system that transmits voice calls, text messages, live chat, e-mail, and other methods of communication in an effective manner.

Hamilton also utilizes a trouble ticketing system that provides an audit trail and event updates to all parties in a transparent manner. The trouble ticketing system provides updates to associated parties (e.g. PSAPs and other subscribed stakeholders) in near real time. In addition, Hamilton uses a mass notification method of e-mail and text messaging communication.

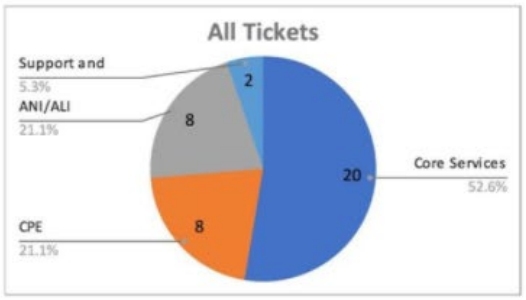
With the Hamilton NOC/SOC also functioning as a help desk, this ensures efficient resolution to open issues regardless of the situation.

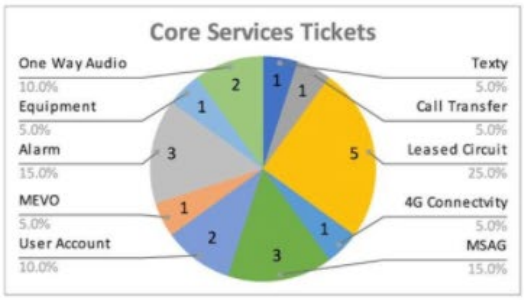
Specific notification intervals are built into the NOC/SOC's operational policy. Currently, the NOC/SOC operates, and complies, with similar SLAs and will not have any difficulty complying with the SLAs detailed within this RFP.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 19.				

Any additional documentation can be inserted here:

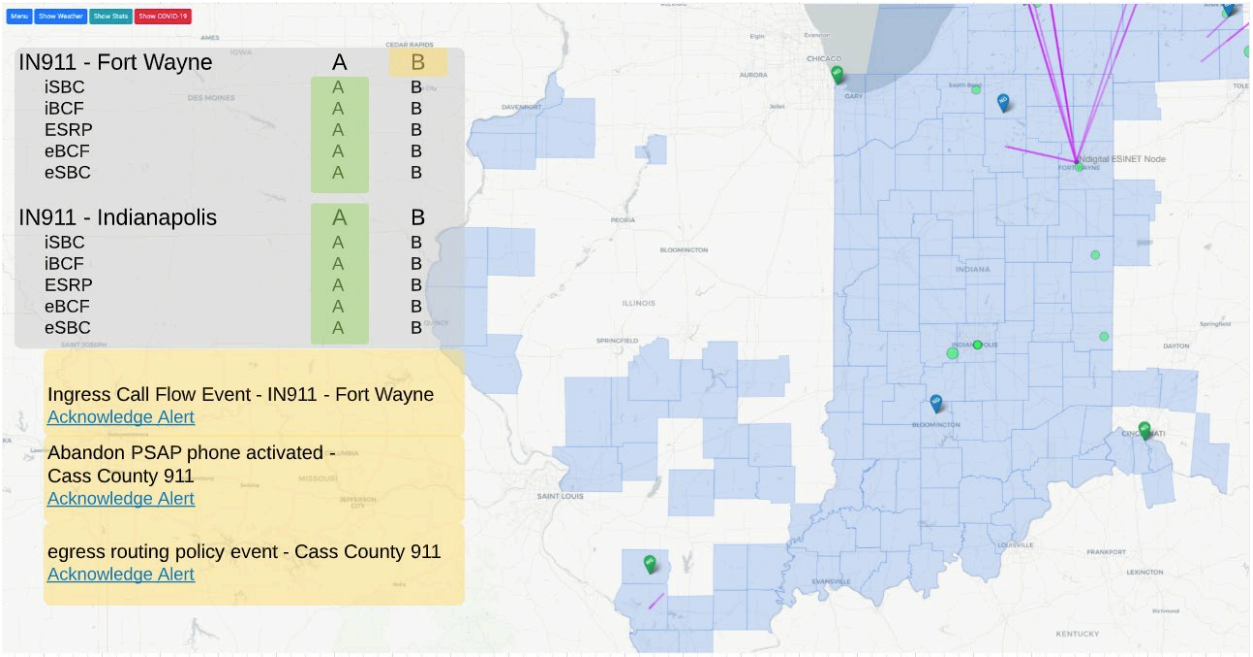
Hamilton will provide an executive dashboard via the NE911.net website. This site will provide the Commission and state PSAPs with access to the content required and near real-time visibility into the facilities and elements that comprise the ESInet. The visibility of network status is displayed geographically with color-coded service impact levels. In addition, the view can be customizable based on the above requirements, as well as other key metrics Nebraska may find beneficial. Hamilton has the ability to provide these in a tabular ticket format, a visual dashboard, or a combination of both formats. The image included below is an example of what Hamilton will provide to the Commission as a component of a regular report. This ticket report details opened, pending, resolved, and closed tickets for a time spanning from 4/12/2020 – 4/18/2020





From 04/12/2020 to 04/18/2020 → 52.6% Core Services Tickets			
Date	Customer	Issue	Date Closed
04/12/2020	[redacted]	101-121-TALLADEGA-MEVO-04 10.205.121.98 Host Check Timed Out	04/14/2020
04/12/2020		101-025-THVLAL-PR01-gi0/0/1 10.205.215.42 Host Check Timed Out	04/13/2020
04/12/2020		101-073-BESSEMERCITY-NG01-AC-FXS 10.205.173.72 Host Check Timed Out	
04/12/2020		CenturyLink circuit outage	
04/12/2020		101-073-AMVLAL-PR02-4G-VPN 10.205.210.31 / Host Check Timed Out	04/16/2020
04/13/2020		All ECW Positions Down	
04/13/2020		Circuit in alarm	04/14/2020
04/13/2020		Mediacom VPN in alarm	04/13/2020
04/13/2020		101-025-GVHLAL-PR01-gi0/0/1 down	
04/13/2020		101-055-GDSDALCTY-PR02-Comcast-VPN is down	
04/13/2020		ETH100-23415649 is down	04/13/2020
04/13/2020		ALI A down 10.HRXZ.5060419 AT&T ticket EJ 066862	04/14/2020
04/13/2020		MTGALDEX-SBC-A and 101-HVLALASC-SBC-A in alarm.	04/13/2020
04/13/2020		ALI bouncing	04/13/2020
04/13/2020		Position 3 in JVILLE hard drive has failed after a power on cycle of PC	
04/13/2020		Anniston PD door phone cutting out almost not understandable	04/15/2020
04/13/2020		Texty cannot be reached.	04/13/2020
04/13/2020		Site CPE Alarms	04/15/2020
04/13/2020		MEVO Changes	04/15/2020
04/13/2020		ALI1 not pingable	
04/13/2020		911 calls with no ALI/ANI	04/13/2020
04/13/2020		IRR at station 3 will not replay	04/13/2020
04/14/2020		Pos 1 time is off 2 hours	04/14/2020
04/14/2020		AL911.net - Contact Form Submission	04/14/2020
04/14/2020		Road update	
04/15/2020		911 call hangs up it shows abandoned and then another call shows up with the sa	04/15/2020
04/15/2020		Reestablish User: Carly Bradley	04/16/2020
04/16/2020		Cannot xfer 911 calls to SO on POS1 and POS2	04/16/2020
04/16/2020		ALI B link bouncing.	
04/16/2020		New street	04/16/2020
04/16/2020		ALI link A down	
04/16/2020		Position 5 Genovation not working	
04/17/2020		ANI failures	
04/17/2020		Needs report for agency	
04/17/2020		Insert into MSAG : Walnut Hill Dr and Walnut Hill Ln	04/17/2020
04/17/2020		NRF/Ghost calls coming in on landline trunk 5, their telco is CL	04/19/2020
04/18/2020		No internet	04/18/2020
04/18/2020		Stuck call	

In addition, the image below depicts an example of dashboard functionality provided via the NE911.net website.

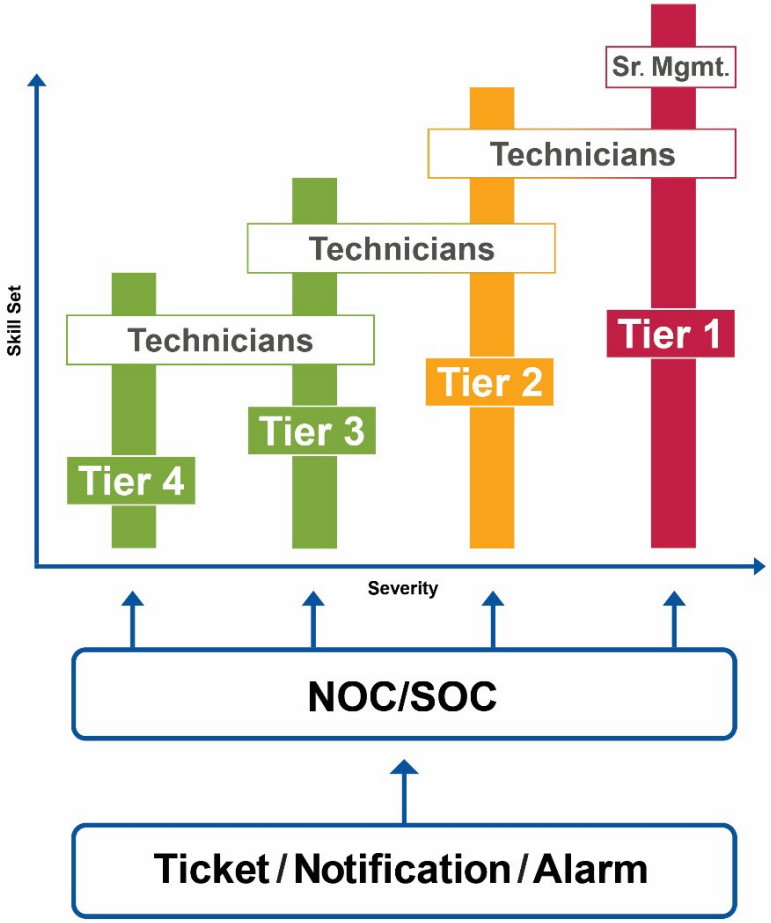


NOC/SOC 20	**NOC/SOC - Escalation Procedures** 1. Outline a detailed regional-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. 2. Describe how discrepancies in the perception of service level agreement (SLA) incident 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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 20.				

Any additional documentation can be inserted here:

The following diagram depicts Hamilton's established escalation procedures:

NOC/SOC Escalation Chart



When a service ticket is submitted to Hamilton's NOC/SOC, it is classified and assigned based on severity. Hamilton's NOC/SOC is utilizing the following severity levels for classification:

- Tier 1 = Critical
- Tier 2 = Major
- Tier 3 = Minor
- Tier 4 = Maintenance

Depending on classification, service tickets are then assigned to appropriate staff. In the event of a tier 1 (critical) incident, or an outage scenario, senior management is automatically notified in addition to the appropriate technicians. If service issues could compromise service level agreements (SLA), staff will escalate to senior management via mass notification application. A pre-arranged outage voice bridge will be established to coordinate restoration efforts. Senior management has identified a Media Contact, specified in SLA 21, to execute the pre-defined media communications and stakeholder notification plan.

In the unlikely event of a malicious attack, the response team is expanded to the Executive, CTO, and Security Officer levels, who would be involved in developing and deploying a solution to resolve the issue.

In addition to the 24x7x365 NOC/SOC operation for support documentation and service-related issues, Hamilton provides an "In Case of Emergency" number to escalate critical services issues if the NOC/SOC were to be unreachable. Additionally, Hamilton provides an offsite call center that provides backup call support and escalation services.

Hamilton's escalation plan conforms with industry best practices. Hamilton follows the Information Technology Infrastructure Library (ITIL) for continuous service improvement as part of its organizational culture. Additional, Hamilton

follows the National Institute of Standards and Technology (NIST) and NENA's next generation 9-1-1 security (NG-SEC) standards and best practices. The industry sees new actors and evolving vectors every day, thus our security posture takes a holistic approach always evolving to match with its environment. As the systems are changed and refined, this will be reflected in the supporting "living" documents.

Hamilton will provide a designated help desk for the Nebraska NG 9-1-1 project, acting as a central point for all communications for the PSAPs. The help desk will also serve as the Hamilton team's central point of contact for maintenance, warranty, and support operations; coordinating and facilitating communication among Hamilton's partners, subcontractors, vendors, equipment manufacturers, and any other entities involved in maintenance operations.

The Hamilton help desk will be in the same facility as the NOC/SOC, ensuring Nebraska with the benefit of reduced reaction time and improved communication as the help desk and NOC/SOC personnel will coordinate efforts and response actions. In addition to managing open tickets, the help desk can serve more broadly as Nebraska's customer service center, center of program operations, liaison between the PSAPs, technical staff, partners and vendors, and additional personnel involved in the project.

The help desk will open tickets for calls received using the existing, field-proven, ticketing system and provide the first tier of technical support by prioritizing, troubleshooting, and isolating problems. When required, the help desk will authorize and coordinate the dispatch of maintenance personnel and will escalate issues when appropriate.

Hamilton uses a variety of communications methods to ensure appropriate technical staff for escalations are notified. These methods of communication include typical telecom systems, as well as alarms and alerts through email, online messaging systems, and direct messaging software applications to provide internal mass notification.

Overall, Hamilton is very much aware that the escalation of problems is critical to the quality of service provided and is very much committed, and experienced, in providing suburb escalation and support services. Hamilton has documented escalation processes, procedures, and personnel capable of supporting the Nebraska NG 9-1-1 project.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 21.				

Any additional documentation can be inserted here:

Effective May 1, 2017, SSAE 16 has been superseded by SSAE 18. SSAE 18 governs reporting on service organizations (SOC Reports) among other types of attestation engagement. A SOC 1 report would typically be used for reporting on the system of internal controls relating to internal control over financial reporting.

Hamilton will obtain a SOC report over the solution in accordance with SSAE 18 standards from an independent accounting firm.

For risks that are not specifically focused on internal controls over financial reporting, the applicable report option is generally considered to now be a SOC 2 report. The risks covered by a SOC 2 report relate to: Security, Availability, Confidentiality, Processing Integrity, or Privacy. The SOC 2 type 1 report states whether the Offeror's description of the system is accurate and that controls are suitably designed as of a point in time. The SOC 2 type 2 reports expands on the Type 1 to include the operating effectiveness of the Offeror's controls and covers a period of time. The SOC 2 report is a restricted use report and should not be made openly available in order to protect the systems and information.

Hamilton engaged and completed an independent third party (Optiv) NIST 800-53 Assessment in the 2016/2017 time frame and, upon request (but, not as part of a public document), Hamilton would provide relevant sections of that Assessment for review. Hamilton has recently engaged Optiv for an updated NIST 800-53 Assessment which is

substantially complete at this point and, upon request (but, not as part of a public document), Hamilton would provide relevant sections of that Assessment for review. Upon contract award, Hamilton would recommend that the State and Hamilton, utilizing NIST 800-53, the NIST Cybersecurity framework, 9-1-1 industry best practices and SOC Readiness Assessment Tools, agree to classify and select appropriate controls for the NG 9-1-1 systems and data. Hamilton will then provide a SOC report to the State demonstrating that its solutions have been implemented with the necessary controls. The agreed upon audit type (i.e. SOC 1, 2, or 3 and Type 1 or 2) or controls can then be determined and audited at an agreed upon interval. Hamilton would also be willing to agree to a customized SOC report to ensure the most efficient and effective type of audit is utilized to ensure that the appropriate controls are in place.

Trust Service Criteria (TSC) was established by the Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accounts (AICPA) to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and system across either ran entire entity; at a subsidiary, division, or operating unity level; within a function relevant to the entity's operational, reporting, or compliance objectives; or for a particular type of information used by the entity. In order to appropriately prepare for the completion of a future SOC report, Hamilton has completed a Trust Services Criteria (TSC) Self-Assessment. This assessment illustrates the principals/criteria evaluated and confirms Hamilton has appropriate controls in place. Please see Appendix 9 – 2020 Trust Services Criteria (TSC) Self-Assessment.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NOC/SOC 22.				

Any additional documentation can be inserted here:

Routine & On-Demand Back-Ups

Hamilton provides for the day-to-day operational archiving as outlined above. Different critical elements use different archiving strategies. Some systems archive in real time 24x7, while other lower priority archiving may be archived daily. Each functional element provides the ability to manually create an on-demand backup of system configuration. A backup or archived configuration file can be manually restored by a system administrator. '

Managing the Configuration Backup & Restoration Processes

Archives are kept in market and in multiple operating nodes on the ESInet, as well as offnet at datastores throughout the United States and in secure cloud storage locations. Comprehensive network segmentation of data archiving will be used and tagged at a lower quality of service (QoS) priority than voice and data for payload 9-1-1 services.

During network restoration, the top priority is restoration of service. Hamilton operations policy dictate that any incident affecting three or more PSAPs or an event involving three or more technicians be immediately communicated company-wide.

As a first step after notification, a conference bridge is initiated to allow technical resources and troubleshooting to be coordinated. At this point a Public Information Officer (PIO) is appointed to manage communications to affected customers and other interested parties.

Technical resources are coordinated via the conference bridge to optimize troubleshooting efforts. The conference bridge will remain open until service has been restored. Overall, Hamilton's processes and procedures provide the ability to manage configuration backup and restoration processes in a manner that has no negative impact on the Commission's ESInet and NGCS solution.

Continuity of Operations (COOP)

Hamilton's proposed solution includes a defined continuity of operations plan (COOP) and Hamilton is committed to working collaboratively with the Commission to create and implement the most efficient and responsive plan possible. Within this response, Hamilton has provided best practices for a COOP and will complete a comprehensive evaluation of the customer site upon contract execution.

Hamilton's COOP ensures that all critical NG 9-1-1 services and NGCS functions can provide similar functions using alternative means in the wake of a disruption and after a disruption has been recognized.

Specific to the NGCS and delivery of 9-1-1 traffic via the IP network to the respective host locations, Hamilton utilizes diverse data centers, including the Nebraska Data Center (NDC) and Hamilton's established data center in Aurora, NE. This design foundation includes geographically diverse data centers that operate in an active/active configuration. There are no hot sites, warm sites, and cold sites. All facilities are processing traffic and have the capabilities to handle all of the traffic for the Nebraska NG 9-1-1 project providing true geographic redundancy and resiliency.

In addition, Hamilton's ESInet provides the foundation for the functional elements and transports the calls to the host locations. This network is redundant and resilient by design as Hamilton provides redundant facilities and those facilities will be diverse by carrier where available. This prevents the service interruption due to transport provider network and technology.

The functional elements responsible for routing the 9-1-1 traffic has multiple layers of redundancy within itself. Overall, Hamilton ensures there are safeguards to defend against exposure to any single point of failure and to ensure continuity of service.

Hamilton's proposed solution includes the optional use of the MEVO(+) service as part of the continuity and disaster recovery system. MEVO(+) is designed to ensure delivery of calls and automatic location information (ALI) to the PSAP in the event of an impairment of the NGCS, ESInet or primary 9-1-1 call handling solution. The NGCS nodes use the policy routing function (PRF) to automatically reroute calls to the MEVO(+) system in the event of a system impairment or failure. This can also be accomplished at the individual Regional Call Host (RCH), or PSAP level, at the at the host locations, at the regional level, or on a statewide level. Calls can be automatically re-routed to another PSAP, a mobile command center, or the MEVO(+) platform by the PRF function.

Alternatively, PSAPs may request that calls be redirected to MEVO(+) by calling the network operations center/security operations center (NOC/SOC), or by activating the 'abandon PSAP switch' by the local authority. This is useful in accommodating scheduled maintenance activities at the PSAP. When calls are redirected to MEVO(+) at the PSAP level, MEVO(+) is deployed as a separate VoIP phone at each workstation. The phones are registered over the ESInet to the MEVO(+) server.

If the Commission opts to utilize the optional MEVO(+) service, specific RCH Contingency Plans will be negotiated with each RCH as part of the ESInet onboarding process. These plans will include action plans for RCH busy scenarios, RCH unavailable scenarios, bug out scenarios, or routine maintenance scenarios.

Additional information about Hamilton's COOP is provided in requirement NOC/SOC 1 and more specific information about Hamilton's MEVO(+) disaster recovery platform can be found in requirements SLA 18 and ESI 8.

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			
	Bidder Response: Hamilton complies with requirement NOC/SOC 23.				

1. In support of the Commission's consideration of such an option, bidder shall indicate the compliance level of 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			

Any additional documentation can be inserted here:

The Hamilton solution is capable of supporting third-party NOC/SOC integrations and, as detailed above in Section 5.1.5, the following chart shows Hamilton's compliance level in providing access to third-party NOC/SOC overarching support. The Hamilton Service model is a fully integrated service where the NOC/SOC functions are fully engaged and integrated into the provisioning of service. Separating the ESInet services from the NOC/SOC service is technically possible and Hamilton would support that if desired. However, Hamilton strongly encourages consideration be given to utilizing our integrated service for the highest grade of service.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 1.				

Any additional documentation can be inserted here:

Capacity Levels

Hamilton commits to provide the required capacity needs to ensure the ability to grow current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. Hamilton's next generation core services (NGCS) nodes are scalable and have the capacity to far exceed the growth requirements of the project.

Hamilton is proposing a purpose-built NG 9-1-1 network and managed services solution to meet the performance and availability requirements dictated by the Commission and the capacity demands of the state of Nebraska. This proposed solution includes both next generation core service (NGCS) nodes and an ESInet transport design that exceeds the total design capacity for the state. Hamilton intends to use Nebraska Link as the underlying transport network to provide connectivity to the Regional Call Hosts (RCH). This will allow Hamilton to acquire and provision transport from all relevant local providers. IP connectivity will be scaled to meet the requirements of each RCH, but will not be less than 200Mbps at each RCH. Hamilton expects this additional bandwidth will allow considerable flexibility for the state as it looks at possible growth of call taker positions and/or the addition of new services, such as multimedia texting (SMS).
The core call processing nodes will be in the following two datacenters:

- Hamilton Data Center – 1006 12th Street, Aurora, NE 68818
- Nebraska Data Center (NDC) – 1623 Farnam Street, Omaha, NE 68102

These two data centers will provide redundancy for the core nodes. We are proposing that each RCH have redundant dedicated IP connections, one connection to each call processing node, as well as a tertiary connection that utilizes either commodity IP or wireless 4G/LTE connectivity.

NGCS nodes process both voice and non-voice media. Each node is capable of processing over 1,000 simultaneous SIP sessions. Peak processing on a production system has been tested to 14,000 sessions per second. Therefore, the call processing nodes are capable of processing call loads much greater than the historical call volumes for Nebraska. In lab testing, the SIP:ME routing core, which comprises the BCF and ESRP functions, has been shown capable of sustaining call loads greater than 50,000 calls per hour.

Hamilton's solution design permits scalability as the NGCS call processing elements are deployed in a virtual machine (VM) environment, providing the ability to add resources as required. Software licensing is commonly based on the population of a state/region/municipality. For the purpose of this proposal, software licensing would be based on the population of the state of Nebraska. After the project is successfully implemented, the only variance in charges would be related to price-per-population adjustments associated with population increases or decreases.

Hamilton is also responsible for the network planning and forecasting and will engineer the ingress ESInet capacities based on these requirements.

Hamilton's preferred network design is to utilize the highest quality network providers in each core site, PSAP, or region to develop the most reliable network. For the completion of the Nebraska NG 9-1-1 project, Hamilton will utilize Nebraska Link's state-of-the-art fiber optic network throughout the state of Nebraska. The primary network connections will be 100% fiber connections. Hamilton's design will also utilize IP connections from local internet service providers for secondary network connections in some locations. The potential technologies include cable modem, DSL, 4G/5G wireless, fiber, and close to any other transport method to create an ESInet with the priority for the secondary connection being to utilize a wired (direct fiber, DSL or cable modem). Utilizing multiple network providers and facilities, rather than utilizing a single provider for both the primary and secondary network connections, will maximize both the diversity and redundancy of the call routing.

In addition, by utilizing border gateway protocol (BGP), bi-directional forwarding detection (BFD), and other open shortest path first (OSPF) routing protocols, we propose to create a self-healing, scalable network. If additional bandwidth or additional survivability is required to maximize scalability and/or diversity of routes, it is simple to add additional network connections.

The ESInet will use redundant 1Gbps connections between the data centers. The router ports on the core-to-core connections are capable of multiple 1 Gbps connections and would not require a hardware change in the event of increased bandwidth requirements. Hamilton has not experienced capacity constraints for transport speeds in excess of 1Gbps for deployments of more than ten times the population and call volumes of Nebraska's current volumes.

Lead Times

Within this RFP response, Hamilton has contractually secured the ability to increase any IP component necessary to increase capacities with no additional contractual paperwork. In order to increase capacities on each element of the IP network, Hamilton will need approximately five (5) days to increase a Regional Call Host (RCH) circuit and 14 days to increase a core to core circuit. Hamilton's core elements have been capacity tested to over 10,000 calls per hour in pre-production testing. Bandwidth calculations at this call rate equate to approximately 2 megabytes of sustained voice traffic across the network.

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 2		X			
	Bidder Response: Hamilton complies with requirement SLA 2.				

Any additional documentation can be inserted here:

The Hamilton ESInet will be designed to operate with less than 50 ms of latency

Hamilton utilizes a "pitcher-catcher" method of sending packets through the network to actively determine network quality. This testing is unobtrusive and can be conducted either continuously or at regular intervals. For example, SLA measurement could be the average latency per hour based on samples taken every one (1) minute. The results are captured by a suite of tools utilized by the network operation center/security operation center (NOC/SOC) and logged. Reports for any interval can be created and provided to the Commission as reasonably requested and agreed upon by Hamilton and the Commission.

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 3		X			
	Bidder Response: Hamilton complies with requirement SLA 3.				

Any additional documentation can be inserted here:

The proposed solution is designed to provide a maximum latency between points of interconnection of less than 60 ms 99.9% of the time and less than 100 ms 99.999% of the time. It is best practice to design ESInets to operate with less than 15 to 20ms of latency, which allows the functional elements to encode and decode and a conference bridge in the middle of the path and still achieves the maximum 37ms or less packet delay. This information is gathered, logged, and reported via a suite of administrative tools utilized by Hamilton's NOC/SOC. Hamilton suggests a one (1) minute sample interval, but will work with the Commission to negotiate a reasonable interval for calculating latency figures. Latency reporting will be provided to the Commission as reasonably requested and in scheduled reporting intervals as agreed upon by Hamilton and the Commission.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 4.				

Any additional documentation can be inserted here

It is best practice to design ESInets to operate with less than 15 to 20ms of latency, which allows the original to encode and decode and a conference bridge in the middle of the path and still achieves the maximum 37ms or less packet delay. The proposed solution is designed to provide a maximum latency between points of interconnection of less than 60 ms 99.9% of the time and less than 100 ms 99.999% of the time. This information is gathered, logged, and reported via a suite of administrative tools utilized by Hamilton's NOC/SOC. Latency figures will be provided to the Commission as reasonably requested and in scheduled reporting intervals as agreed upon by Hamilton and the Commission.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 5.				

Any additional documentation can be inserted here

Hamilton's proposed solution is designed to deliver a Mean Opinion Score (MOS) of 4.0 or better.

MOS is a traditional measure of voice quality and originates from a process of using human evaluators to rate sound quality.

Hamilton's proposed solution utilizes a "pitcher/catcher" system to constantly measure path and delivery success of test packets through the network. The monitoring system included in the proposed solution utilizes probes placed at each Regional Call Host to capture information as it ingresses and egresses the network, providing the underlying data to substantiate MOS scoring and SLA compliance reports for the ESInet. The monitoring platform provides alerts and notifications to the network operation center/security operation center (NOC/SOC) of packet delivery failures, which might result in decreased MOS. This measurement tool will be especially important in determining SLA compliance when the human MOS judgment could be influenced by Regional Call Host (RCH) to PSAP network elements that are out of Hamilton's control. Further, this ensures timely and proactive troubleshooting of any potential problems, resulting in the delivery of an average MOS of 4.0.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 6.				

Any additional documentation can be inserted here

Hamilton actively monitors packet loss on all network segments and believes it is best practice to engineer the ESInet to keep the packet loss budget under 1%. Real-time or circuit history is available to ensure SLA compliance. Hamilton actively monitors packet loss on all network segments and real-time or circuit history is available to ensure SLA compliance. This information is gathered, logged, and can be provided to the Commission and affected PSAPs as requested.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 7.				

Any additional documentation can be inserted here

Hamilton will meet the total packet latency requirement of less than 50ms of latency between the data centers and the Regional Call Hosts (RCH). Hamilton will actively monitor core-to-core and core-to-RCH latency on all network segments.

Hamilton's proposed solution utilizes a "pitcher/catcher" system to constantly measure path and delivery success of test packets through the network. The monitoring system included in the proposed solution utilizes probes placed at each PSAP to capture information as it ingresses and egresses the network, providing the underlying data to substantiate network latency scoring and SLA compliance reports for the ESInet. The monitoring platform provides alerts and notifications to the network operation center/security operation center (NOC/SOC) of packet delivery failures. Reports for any interval can be created and provided to the Commission and affected PSAPs as agreed upon between Hamilton and the Commission.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 8.				

Any additional documentation can be inserted here

The proposed solution is designed and engineered to operate with an average jitter of less than 30ms. Hamilton is prepared to provide qualitative data showing that our existing ESInet deployments have produced high quality voice networks with jitter </= 30ms.

As detailed earlier, Hamilton's proposed solution utilizes a "pitcher/catcher" system to constantly measure path and delivery success of test packets through the network, including jitter measurements. The monitoring system included in the proposed solution utilizes probes placed at each Regional Call Host (RCH) to capture information as it ingresses and egresses the network, providing the underlying data to substantiate jitter scoring and SLA compliance reports for the ESInet. The monitoring platform provides alerts and notifications to the network operation center/security operation center (NOC/SOC) of packet delivery failures. This information is collected and logged. Reports for any interval can be created and provided to the Commission and affected PSAPs as agreed upon between Hamilton and the Commission.

SLA 9	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SLA 9.				

Any additional documentation can be inserted here

Hamilton's solution will have a network traffic convergence of less than 54 milliseconds (ms) and makes use of industry standard protocols to meet this requirement. Hamilton is prepared to provide qualitative data showing that our existing ESInet deployments have produced high quality voice networks with network convergence less than 54ms. The following two routing protocols are combined to ensure the specified availability: (1) bi-directional forward control (BDF) and (2) enhanced interior gateway routing protocol (EIGRP). This information is collected and logged. Reports will be generated and provided to the Commission and affected PSAPs as requested.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SLA 10.				

Any additional documentation can be inserted here

The functional elements contained in this solution are configured to be redundant in an active-active configuration. This design helps to ensure continuity of service in the event of a functional element (FE) impairment. Our design goal is to ensure continuity of service to the Regional Call Host such that no single functional element (FE) impairment would disrupt service.

In the event of the failure of a FE, mean time to repair (MTTR) is calculated by review of logs from both the FE and the monitoring system. By reviewing the notifications and logs generated by the monitoring system and comparing that data to FE log data, the Commission and Hamilton can determine the beginning time of an event and the ending time of that event. MTTR will be defined as the difference between the beginning and ending log events. This calculation represents the MTTR for the affected FE and is not necessarily indicative of a service impairment.

The same methodology would be applied in an impairment event impacting the delivery of a service. A Root Cause Analysis (RCA) is conducted after any significant network event and these reports are made available to all affected PSAPs and the Commission. MTTR reports will be provided to the Commission and affected PSAPs as reasonably requested and in scheduled reporting intervals as agreed upon by Hamilton and the Commission.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SLA 11.				

Any additional documentation can be inserted here

The proposed solution is designed to provide a 99.999% uptime service level. The active-active configuration of the functional elements (FE) allows a redundant FE to immediately takeover in the event its mated FE experiences an impairment. All hardware, software, and network elements are installed and configured in a redundant and resilient manner.

This configuration is also advantageous in a planned maintenance scenario. A single FE can be taken out of service while its redundant mate continues to provide its function. This capability allows the mean time between failures (MTBF) to be extended almost indefinitely. The solution is designed to operate with no planned outage of service.

In the event of a failure, logging data from both the monitoring system and the FEs will be collected and compared to determine the start and end times of a failure. MTBF reports will be provided to the Commission and affected PSAPs as reasonably requested and in scheduled reporting intervals as agreed upon by Hamilton and the Commission.

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 12		X			
	Bidder Response: Hamilton complies with requirement SLA 12.				

Any additional documentation can be inserted here

As detailed throughout this RFP response, Hamilton's design approach eliminates single fault domains through the use of redundant and diverse network elements and transport segments. System reliability and availability are critical components within the proposed solution architecture by Hamilton. The solution design is sized to handle all 9-1-1 calls and payloads regardless of independent equipment failure, data center failure, ESInet failure, RCH failure, or WAN failure. Redundancy and diversity are key elements contained in the Hamilton solution.

Hamilton's proposed system, including all subsystems, will be available a minimum of 99.999% of the time when measured on a 24x7x365 basis during a calendar year. The solution design is carefully considered through the use of geographic diversity, as well as physical and virtual redundancy. The Service Level Agreement (SLA) is intended to be consistent with the recommendations of ESIND and NENA-STA-010.2-2016.

Network availability calculations will be calculated monthly and will include scheduled and routine maintenance. Any services or components that will be taken offline for maintenance will be communicated to involved parties by the 9-1-1 network operations center/security operations center (NOC/SOC).

	Service Level Agreements - System Performance **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
SLA 13		X			
	Bidder Response: Hamilton complies with requirement SLA 13.				

Any additional documentation can be inserted here

Uptime Definition

Hamilton is defining uptime using the mathematical formula on page 34 of *NENA-INF=016.2-2018 (dated April 5, 2015)*, as follows:

Availability = *UpTime / (UpTime + DownTime)*

	YEARLY	MONTHLY	DAILY	HOURLY
99.999% ("five nines")	5.26 minutes	26.30 seconds	6.05 seconds	864.00 milliseconds

The data below illustrates uptime calculations for ESInets utilizing the same core technology.

LOCATION	SERVICE HOURS (CONTRACT TO DATE)	UPTIME PERCENT
Alabama	19,464	99.9999% ("Six Nines")
New Hampshire	41,856	99.9998% (greater than "Five Nines")

All network elements and functional elements are deployed in parallel in the proposed solutions.

In-market MTBF (observed) for functional elements in the proposed solution:

DESCRIPTION	QUANTITY	MTBF
LNG Node	2	10 years
NGCS Node	2	5 years
MEVO Node	4 to 8 years	5 years
IP Core Routing Notes	2	10 years
RCH / PSAP Routers	2 (per RCH / PSAP)	5 years
RCH / PSAP Firewalls	2 (per RCH / PSAP)	5 years

The proposed solution also includes national nodes in two geo-diverse locations. These serve as additional N+1 redundant functional element. This design objective forms a fully redundant system for the in-market nodes.

Additional redundancy for the proposed solution is provided by this parallel design.

Edge (RCH/PSAP) hardware is proposed to be replaced every five years, and network element or functional element components are expected to age out during the contract period.

DESCRIPTION	QUANTITY	MTBF
LNG Node	4	10 years
NGCS Node	4	5 years
MEVO Node	4	5 years
IP Core Routing Notes	2	10 years
RCH / PSAP Routers	2 (per RCH / PSAP)	5 years
RCH / PSAP Firewalls	2 (per RCH / PSAP)	5 years

All sites will be within two hours' drive time of a service technician. Spare equipment will be located at the NGCS nodes and with the technicians so that there are no additional lead times to obtain the replacement equipment before commencing travel for a troubleshooting event. With Hamilton, and its subcontractor Nebraska Link, a multitude of technical staff will be located in Nebraska for remediation of trouble events.

Mean Time to Restore (MTTR) = (Total Maintenance Time) / (number of repairs)

The chart below illustrates MTTR measurements.

MINUTES TO RESTORE	NUMBER OF REPAIRS	MTTR
30	1	30
60	2	30
90	3	30
120	1	120
150	1	150

As proven by the Alabama and New Hampshire data, the overall availability of services is expected to meet, and exceed 99.999% for the duration of the contract. Availability of system and critical hardware will be included in reporting requirements defined by the Commission.

System Availability Information

As stated throughout this section, the Hamilton design approach eliminates single fault domains through the use of redundant network elements and transport segments. System reliability and availability are critical components within the proposed solution architecture by Hamilton. The solution design is sized to handle all 9-1-1 calls and payloads regardless of independent equipment failure, data center failure, ESInet failure, PSAP failure, or WAN failure. Redundancy of elements and diversity of routing are key elements contained in the Hamilton solution.

The solution design is carefully considered using geographic diversity, as well as physical and virtual redundancy, to ensure a total system availability of 99.999%, as defined in NENA-INF-016.2-2018. Hamilton can demonstrate that the proposed solution is engineered to maximize uptime and availability.

Network availability calculations will be calculated monthly and will include scheduled and routine maintenance and LAN/WAN interfaces, including the call handling subsystem, logging and recording subsystem, OSP external interfaces/WANs, and land mobile radio (LMR) interface. Any services or components that will be taken offline for maintenance will be communicated to involved parties by the 9-1-1 network operations center/security operations center (NOC/SOC).

Statseeker Professional

Interface Availability

Thu 18 Oct 2018, 10:50 (America/Indiana/Indianapolis)

Sat Sep 1 00:00 2018 to Mon Oct 1 00:00 2018 America/Indiana/Indianapolis

Totals (SLA Transitions: 0, SLA Outage Time: 0secs, Transitions: 0, Outage Time: 0secs) Averages (SLA Availability: 100.00%, Availability 100.00%)

Device	Interface	SLA Availability	SLA Transitions	SLA Downtime	Availability	Transitions	Downtime
133-013-CNCDNH-ASR1	Gi0/0/10.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/1.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Te0/0/12	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/2	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/0	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/5	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Te0/0/13	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/3.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	BD2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/7	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/4.SI.4000	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/8	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/9	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/3	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/10	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/6	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/2.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/11	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/4	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/5.SI.4000	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/6.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/7.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/1	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s

24 of 24 interfaces displayed

Above, is an example of an availability report for all interfaces on next generation core service (NGCS) switch ASR1 located in Concord, New Hampshire.

In addition, Hamilton will provide a monthly state level report including a statement of service availability and trouble ticket analysis. A sample state level report can be found in Appendix 10 - ANGEN NG 9-1-1 Report for the Reporting Interval Ending January 6, 2019.

		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: Hamilton complies with requirement SLA 14.				

Any additional documentation can be inserted here

The proposed service is an all-inclusive "9-1-1 as a service" model. Therefore, Hamilton will be responsible for all costs associated with all hardware, software, and applicable services replacements whether the cause is due to end-of life by the manufacturer, a product is defective or unserviceable due to failure or malfunction, or an upgrade is deemed necessary to maintain continuity of operations. All equipment utilized to provide the service will be of new or current manufacture and not refurbished. Any equipment reaching end of life will be replaced more than 90 calendar days prior to the manufacturer's end of support (EOS) date.

		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: Hamilton complies with requirement SLA 15.				

Any additional documentation can be inserted here

Hamilton has developed processes and procedures for supporting a NOC/SOC that can rapidly triage and manage reported network incidents. These processes and procedures include advanced monitoring solutions and TeamSupport ticketing. Hamilton's TeamSupport ticketing solution can support multiple SLA's and escalation procedures. An example of this type of process is illustrated below.

Support requests are manually entered via the web interface and/or auto generated by maintenance tools. Notifications are then distributed to the appropriate distribution list based on pre-defined requirements. An offsite call center, providing backup call support and escalation services, is also available in the event the Primary NOC/SOC were unreachable. Additionally, Hamilton provides an "In Case of Emergency" number to escalate critical services issues if the primary and secondary NOC/SOC were to be unreachable. Any ticket submitted electronically or created by the NOC/SOC is assigned a support representative and managed within 15 minutes. If a ticket is not assigned within 15 minutes, notice is sent to NOC/SOC managers and executive management.

Depending on classification, service tickets are then assigned to appropriate staff. In the event of a tier 1 (critical) incident, or an outage scenario, senior management is automatically notified in addition to the appropriate technicians. If service issues could compromise service level agreements (SLA), staff will escalate to senior management via mass notification application and effort to restore service is immediate and sustained, 24x7, until a final resolution is in place. A pre-arranged outage voice bridge will be established to coordinate restoration efforts and critical service restoration is expected to start immediately with updates provided every hour, unless escalated to outage scenario.

The Media Contact will execute the pre-defined media communications and stakeholder notification plan. In the unlikely event of malicious attack, the response team is expanded to the Executive, CTO, and Security Officer levels, who would be involved in developing and deploying a solution to resolve the issue.

In contrast to a tier 1 (critical) incident, high priority work is expected to be completed within four hours and low priority, or normal priority, tickets requiring scheduled non-critical in-field support is expected to be scheduled and performed within five business days.

When a service ticket is submitted to Hamilton's NOC/SOC, it is classified and assigned based on severity. Hamilton's NOC/SOC is utilizing the following severity levels:

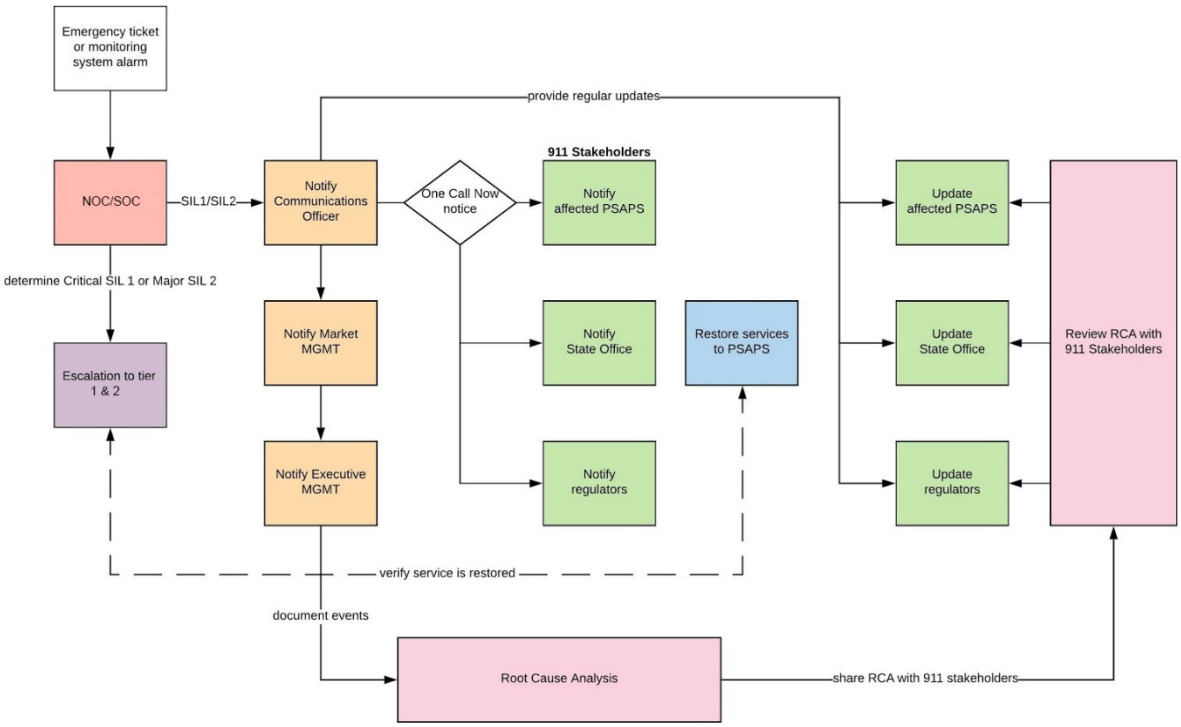
- Tier 1 = Critical
- Tier 2 = Major
- Tier 3 = Minor
- Tier 4 = Maintenance

Below, Hamilton has included an example of a service matrix. This service matrix provides a description of incidents and time frames for ticket initiation, updates, communication methods, and restoration as recommended by Hamilton. However, Hamilton is willing to negotiate the components of this service matrix as reasonably required by the Commission, the Regional Call Hosts (RCH), and the PSAPs.

SERVICE LEVEL IMPACT	INCIDENT TYPE	COMMUNICATION METHOD FROM SERVICE PROVIDER TO CUSTOMER (all listed methods)	TICKET INITIATION	UPDATE FREQUENCY (e-mail)	RESTORATION NO LATER THAN
Tier 1 - Critical Full loss of critical functionality	Trunk outages, Alternative Routing Activation, All calls misrouting, No ANI/ALI, Loss of service, FCC reportable incidents, PSAP unable to perform core functions, Transfer failures (all calls), Circuit outage, Ransomware or Malware attack	Phone Text Email	≤15 minutes	≤1 hour	≤4 hours
Tier 2 - Major Partial loss of critical functionality	Intermittent misroutes, Intermittent transfer failures, Intermittent ALI issues, no/incorrect data, WAN links bouncing intermittently, Inability of PSAP to support 9-1-1 calls due to equipment failures	Phone Text Email	≤30 minutes	≤2 hours	≤8 hours
Tier 3 - Minor	Occasional calls	Phone	≤1 hour	≤24 hours	≤7 calendar days

Does not have serious impact	Misrouting occasional transfers to other PSAPs failures, PSAP equipment issues that do not impact call taker response	Email			
Tier 4 - Maintenance Does not have serious impact or informational	Non-Critical and informational request Maintenance Activities	Email	≤2 hours	≤weekly	≤30 calendar days

For service affecting issues, a root cause analysis (RCA) is performed to determine why service was affected and what will be done to prevent a system impairment in the future. A comprehensive report is created and shared with stakeholders. Additional explanation, presentation, and analysis are typically performed in coordination with the State. Hamilton's communication flow chart is detailed below.



In the event a critical ticket or monitoring system detects a system failure:

- NOC/SOC validates problem and escalates to tier 1 & 2 technical staff.
- NOC/SOC notifies Communication Officer (typically Market Manager or Executive Management).
- Communication Officer utilizes mass communication (One Call Now) system to communicate potential problem via text, direct call, and email.
- NOC/SOC triages support calls.
- Tier 1 & 2 continue to restore services.
- Communication Officer creates timeline, document calls, alarming, and troubleshooting efforts.
- Communication Officer provides updates via the One Call Now (OCN) platform.
- Communication Officer provides all clear from OCN.

- Provides direct communication to state office and regulators of root cause timelines.
- A draft Root Cause Analysis (RCA) is shared with the state to validate comprehensive report.
- RCA report is shared system wide and review meetings are held to address questions and answers.

Critical and major service issues will have direct communication by executive management and/or in-market state managers. Hamilton's NOC/SOC monitors all network elements, functional elements, and the interfaces that are the point of interconnection (POI) with other entities.

Hamilton will work with the Regional Call Host PSAPs to identify and create lists of contacts and groups pertinent to the various classifications of events, escalations, and resolutions.

As mentioned within this response, Hamilton utilizes a One Call Now (OCN) notification system that transmits voice calls, text messages, live chat, email, and other methods of communication in an effective manner. This platform is utilized to provide network status alerts, notification of emergency network events, or outages. Contact lists shall be provided by the local stakeholders and Hamilton technicians will enter the information into our helpdesk Software, TeamSupport, and the OCN platform in order to maintain a current communication list.

Within the OCN environment, we provide two classes of notification categories:

A. A Broadcast Warning Message (BWM) - this class of notification is the highest priority and will include additional operating variances and notifications as required.

B. A Broadcast Advisory Message (BAM) - this class of notification is designed to alert the recipients of non-critical, but important service affecting advisory messages.

In addition, Hamilton's ticketing solution, TeamSupport, offers customizable fields, email integration, workflows, automation, and the ability to associate or relate tickets to one another. TeamSupport provides an audit trail and event updates to all parties in a transparent manner.

Through this automation process and workflow functionality, combined with effective NOC/SOC operating policies and procedures, Hamilton will establish protocols defined by the State for notification based on the location, incident type, and severity level. The trouble ticketing system provides updates to associated parties (Regional Host PSAPs and other subscribed stakeholders) in near real time.

To have early visibility into potential issues, our monitoring systems will provide notification, and will send test calls out of band to determine system availability. To improve the human element of escalation and communication, the company has established policies to clearly define when it is time to respond at the highest level.

Hamilton's escalation plan conforms with industry best practices and will be customized to meet FCC regulations, as well as the operating needs of the state, county, and local stakeholders. Critical and major classified tickets or potential service issues will be monitored closely as SLA compliance and state, or federal communications, could be required. Hamilton follows the Information Technology Infrastructure Library (ITIL) for continuous service improvement as part of its organizational culture. Additionally, Hamilton follows the National Institute of Standards and Technology (NIST) and NENA's next generation 9-1-1 security (NG-SEC) standards and best practices. The industry sees new actors and evolving vectors every day, thus our security posture takes a holistic approach always evolving to match with its environment. As the systems are changed and refined, this will be reflected in the supporting "living" documents.

		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: Hamilton complies with requirement SLA 16.				

Any additional documentation can be inserted here

Hamilton has not had any FCC reportable outage situations that interrupted 9-1-1 service to clients over the past three years, including situations where 9-1-1 calls were not delivered or not delivered to the appropriate PSAP as a result of the issue.

In addition, Hamilton agrees to comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract. The proposed solution for notification will be customized to meet applicable FCC outage and notification rules, as well as the operating needs of the state, county, and federal stakeholders.

		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 subcontractors. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Hamilton complies with requirement SLA 17.				

Any additional documentation can be inserted here

In the event of an outage and/or impairment in service, Hamilton will assign the ticket to appropriate technical staff within 15 minutes. Following the assignment of the ticket, Hamilton will notify the Commission and any impacted PSAPs within 15 minutes of discovering an event or outage that may impact 9-1-1 services. Hamilton will follow all applicable FCC rules regarding outage notification during the duration of the contract ensuring that events meeting criteria for local, state, and federal reporting are completed by Hamilton. Hamilton's proposed solution for notification will also be customized to meet applicable FCC outage and notification rules, as well as the operating needs of the state, county, and federal stakeholders.

Available information useful in mitigating the effects of the event and/or outage will be provided, in addition to name, telephone number, ticket/reference number, and email address at which the service provider can be reached. Hamilton accepts responsibility for collecting data and troubleshooting and reporting on behalf of its suppliers.

Additionally, notifications are provided when service impairments are identified within our network, or those of originating service providers (OSP) connected to the ESInet.

The network operations center/security operations center (NOC/SOC) notifies stakeholders via voice and electronic notification. In critical outage scenarios, top level management is involved to provide stakeholder communication and restoration efforts. In the unlikely event of a longer duration outage, a conference bridge will be deployed for stakeholder organization and communication on a real time basis.

The next generation core services (NGCS) nodes, functional, and network elements, as well as the services they provide, are self-healing from the call taker perspective. On all known failure states, the redundant and diverse systems will be configured to automatically maintain continuity of service. This is accomplished by having all functional elements in the call chain assigned multiple delivery destinations, A and B geographic redundancy, and Hamilton's MEVO(+) disaster recovery platform. Additionally, Hamilton utilizes self-healing routing protocols within the ESInet to re-route IP traffic in the event of a circuit failure.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SLA 18.				

Any additional documentation can be inserted here

Hamilton will communicate updated status information to the Commission and impacted PSAPs no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 9-1-1 service is restored. These updated status reports will include information such as the nature of the outage, the best-known case, the geographic scope of the outage, the estimated time for repairs, and any other information that may be helpful to the management of the impacted operations.

Hamilton's ticketing system is integrated with SLA monitoring and assessment service platforms. Stakeholders that create a ticket, have a ticket merged with the master ticket, or become assigned to the ticket receive all relevant updates and status postings by e-mail. This ensures a single source of information that is consistent to all stakeholders. Any stakeholder can add to the knowledge base of the ticket with a reply. Information or assumptions that may not be accurate will be corrected within the workflow of the ticketing process. Stakeholders that are not in the ticket workflow, or that are unable to process e-mail, will be notified by the NOC/SOC using voice or other non-voice methods of communication.

Statseeker Professional

Interface Availability

Thu 18 Oct 2018, 10:50 (America/Indiana/Indianapolis)

Sat Sep 1 00:00 2018 to Mon Oct 1 00:00 2018 America/Indiana/Indianapolis

Totals (SLA Transitions: 0, SLA Outage Time: 0secs, Transitions: 0, Outage Time: 0secs) Averages (SLA Availability: 100.00%, Availability 100.00%)

Device	Interface	SLA Availability	SLA Transitions	SLA Downtime	Availability	Transitions	Downtime
133-013-CNCDNH-ASR1	Gi0/0/10.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/1.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Te0/0/12	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/2	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/0	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/5	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Te0/0/13	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/3.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	BD2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/7	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/4.SI.4000	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/8	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/9	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/3	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/10	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/6	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/2.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/11	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/4	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/5.SI.4000	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/6.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/7.SI.2522	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s
133-013-CNCDNH-ASR1	Gi0/0/1	100.00	0	0d 00h 00m 00s	100.00	0	0d 00h 00m 00s

24 of 24 interfaces displayed

The effort applied by Hamilton in the event of an outage and/or impairment in service would be immediate and sustained, 24x7, until a final resolution is in place. Hamilton will make all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. Utilizing a temporary workaround solution, such as the 800 number or Hamilton's MEVO(+) disaster recovery platform, public callers will continue to reach the PSAP in the event of an outage and/or service impairment and, additionally, this combination will allow the 9-1-1 dispatcher to continue normal operations with a high level of functionality.

This automatic failover is achieved by border gateway protocol (BGP) and bi-directional forwarding detection (BFD) open shortest path first (OSPF) routing protocols within the ESInet.

Failover call routing from the originating service providers (OSPs) is completed by dual homing the 9-1-1 trunking to diverse and redundant ESInet host sites. These ESInet host sites are located at the two data center facilities, which include the Nebraska Data Center (NDC) and the Hamilton Data Center. In addition, Hamilton provides multiple layers of redundancy and failover for the OSPs to connect to the 9-1-1 network in the event of a trunking failure. These methods include the 800-number failover and, for OSPs with the technical capability, internet-based routing, via VPN connections, similar to the method with which a VOIP provider would route their 9-1-1 calls.

Our 800-number failover provides a backup route to the next generation core services (NGCS) nodes allowing the NGCS nodes to identify the calling party number and process it as automatic identification (ANI). The public caller will reach the emergency service routing proxy (ESRP) FE, which will utilize the ANI of the 9-1-1 caller, if the call is made from a toll-free dialed number identification service (DNIS) trunk. This allows the ESInet FEs to route the 9-1-1 call to the appropriate PSAP.

Additionally, the MEVO(+) disaster recovery platform is designed to deliver automatic location information (ALI) to the PSAP in the event of an impairment of the ESInet or primary 9-1-1 call handling solution. In this scenario, the NGCS nodes use the policy routing function (PRF) to automatically reroute calls to MEVO(+). The rerouting of calls can occur at the individual PSAP level, at the regional level, or the statewide level and this platform maintains an enhanced level of 9-1-1 functionality critical to PSAP operation.

Overall, Hamilton provides these many methods of secure, failover call-taking solutions for PSAPs to ensure that all public callers will reach the PSAP even in the event of a service impairment and that 9-1-1 dispatchers can continue normal operations with a high level of functionalities. Hamilton commits to maintaining communication with the Commission, through the use of a phone or IP-bridge, during the outage and/or impairment incident until the incident is fully resolved and service fully restored.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 19.				

Any additional documentation can be inserted here

A preliminary RFO report will be provided to the Commission and impacted PSAPs following the restoration of normal 9-1-1 service. This preliminary RFO report will be provided no later than three (3) days after discovering the outage. A more detailed RFO, including a root-cause analysis (RCA), will be provided to the Commission and impacted PSAPs within ten (10) calendar days after discovering an outage.

Compliance with RFO Notification & Reporting

As mentioned above, Hamilton preforms a comprehensive analysis of all network events, whether they are critical in nature or minor. This analysis will produce an after-action review, with documented action items that will be shared with qualified stakeholders. This process follows the five Information Technology Infrastructure Library (ITIL) stages of continuous service improvement.

NOC/SOC Tools & Techniques

Hamilton uses a real-time collaborative authoring platform and method of secure shares of these notes, a timeline of events, the findings and actions taken. Shares of this collaborative platform are available to qualified users, with the provision that the RFO working document will be updated and revised as additional facts become known. Hamilton will comply with all other requirements of the RFP related to RCA analysis and reporting.

Hamilton has provided a description of the trouble ticket-based status using the workflow described above. This platform provides full transparency to all stakeholders, and fully meets the requirements of SLA 19.

Hamilton uses all commercially available tools and procedures in addition to analytics platforms it has developed for the finding of facts related to RFO and RCA research and review. Additionally, Hamilton has a number of established protocols and standards of operation that have been refined to meet the stringent requirements of analysis and transparent reporting.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 20.				

Any additional documentation can be inserted here

Hamilton strongly agrees that outage notification and follow-up analysis of outages are a critical element to understanding the system's overall health, in addition to preventing future service interruptions. An awareness of issues occurring in a neighboring Regional Call Host (RCH) can provide valuable insight into potential issues that may begin impacting another PSAP's operations.

Therefore, Hamilton's NOC/SOC will serve as the central role as a source of status and additional information and utilizes a notification and reporting system that transmits voice calls, text messages, live chat, e-mail, and other methods of communication in an effective manner.

Hamilton also utilizes a trouble ticketing system that provides an audit trail and event updates to all parties in a transparent manner. The trouble ticketing system provides updates to associated parties (e.g. PSAPs and other subscribed stakeholders) in near real time. In addition, Hamilton uses a mass notification method of e-mail and text messaging communication.

With the Hamilton NOC/SOC also functioning as a help desk, this ensures efficient resolution to open issues regardless of the situation.

As mentioned above, Hamilton offers a number of tools to support PSAP and outage notifications. While it is our preference to manage notifications via our trained NOC/SOC staff, Hamilton's web portal provides authorized users with the ability to select/deselect outage notifications.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SLA 21.				

Any additional documentation can be inserted here

Media Contact

Hamilton has an established public relations policy and will provide a 24x7 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 deliver to the Commission's host equipment and to affected PSAPs. Hamilton's designated media contact for any outage or service failure is listed below:

NAME	PHONE – DIRECT	PHONE – MAIN	CELL	EMAIL
Jim Ediger	402.694.7267	402.694.5101	402.694.1111	Jim.ediger@hamiltontel.com

Government & Regulatory Contact

As mentioned in the previous requirement, Hamilton has an established public relations policy. Hamilton will provide a 24x7 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 affected PSAPs. Hamilton's designated government and regulatory contact for any outage or service failure is listed below:

NAME	PHONE – DIRECT	PHONE – MAIN	CELL	EMAIL
Jim Ediger	402.694.7267	402.694.5101	402.694.1111	Jim.ediger@hamiltontel.com

Hamilton's media and government and regulatory contact, Mr. Ediger, holds a background in legal, regulatory, and telecommunications advocacy which makes him exceptionally qualified for these roles. Mr. Ediger's resume is included within this response and can be found in Appendix 5 – Hamilton Resumes and References.

		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 22. 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: Hamilton complies with requirement SLA 22.				

Any additional documentation can be inserted here

SLA Violations

Hamilton utilizes industry leading SLAs as a standard component of its solution. Hamilton's standard SLAs provide remedies for failing to achieve service assurance measures. Hamilton will comply with the SLA violation specifications above which state that a SLA violation has occurred when (1) the Contractor fails to meet any single performance level; or, (2) 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 22. Hamilton will provide a monthly SLA violations report to the Commission showing compliance with these SLA violation definitions.

SLA Reporting

The Hamilton ESInet service level agreements (SLA) are measured continuously using monitoring tools operated by our network operations center/security operations center (NOC/SOC). SLA reporting is done on a regularly scheduled basis and can be made available to the Commission on the 10th business day of the month. Further, customer notifications for performance impacting issues are consistent with the service impact levels outlined within these SLAs (Tier 1 through Tier 4).

		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: Hamilton complies with requirement SLA 23.				

Any additional documentation can be inserted here

Hamilton acknowledges the States desire for a high availability Next Generation 9-1-1 solution, with a 99.999%, or better, uptime. It is Hamilton's intent to surpass the goals of the service level agreement (SLA) and understands failure to meet SLAs shall be measured per service-affecting outage with financial remedies assessed for failure to meet SLAs. Hamilton will measure its network facilities, devices, and services on a rolling, 12-month calendar. Hamilton will provide detailed SLA and monitoring tools to verify compliance and system availability for each functional element in the call flow.

Hamilton complies with the financial remedies outlined above and have further detailed those within this paragraph. Hamilton understands that 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. In the event that the resolution period length of time doubles, the discount shall increase to 20 percent (20%) of the MRC. Further, if the resolution period length of time quadruples the initial period, Hamilton understands that 50 percent (50%) of the MRC shall be assessed. This amount related to the damages will be credited to the invoice for the following month immediately following the violation.

As referenced above, Hamilton is defining uptime using the mathematical formula on page 34 of *NENA-INF=016.2-2018 (dated April 5, 2015)*, as follows:

Availability = *UpTime / (UpTime + DownTime)*

Hamilton will support the reporting of the status and operation of the proposed NG 9-1-1 system and services to the Commission for the purposes of measuring and analyzing Hamilton's provided services and the system performance in

support of the operation of the System throughout the term of the Contract. Hamilton operates a reporting and logging system used to log, record, and report on the operation of the system. These logging, recording, and reporting elements will serve as the primary reporting and data collection sources of the system for all 9-1-1 emergency calls and media payload data. Any service affecting incident, as defined in this SLA, may result in adjustments to the monthly recurring service costs paid by the Commission to Hamilton as set out within this requirement.

Hamilton's reporting may occur on an ad-hoc basis or as necessary for problem resolution or restoration of service related to the system, and may include reporting on an hourly, daily, weekly, monthly basis or as directed by the Commission. Formal reporting provided to the Commission will occur on a monthly/quarterly/annual basis with formats to be determined by Hamilton and the Commission. Types of reporting expected by the Commission may include, but are not limited to:

- System related traffic volumes and capacities.
- System transaction totals, aggregates, accumulations.
- System transaction categorizations, types, groups.
- System operations expected vs. unexpected.

Again, Hamilton's proposed system, including all subsystems, will be available a minimum of 99.999% of the time when measured on a 24x7x365 basis during a calendar year and the proposed SLAs within this response are consistent with the recommendations of ESIND and NENA-STA-010.2-2016.

Hamilton will has provided a sample monthly state level report including a statement of service availability and trouble ticket analysis. This sample state level report for Nebraska can be found in Appendix 10 - ANGEN NG 9-1-1 Report for the Reporting Interval Ending January 6, 2019.

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:

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement GEN SCEN 1.				

Any additional documentation can be inserted here

Beginning at 0300, the NOC/SOC will create a ticket and begin investigating the alarms. Given that multiple alarms were received, company policy requires escalation be made and an internal notification sent. By 0330, with additional tickets being received, a conference bridge will be established. This bridge is to be used by technical staff to coordinate troubleshooting. Because PSAPs have not yet reported a service interruption, the focus is to diagnose the incoming alarms.

At 0345 when PSAPs begin reporting a service interruption, the focus of troubleshooting must be changed to restore quality of service to the PSAP. The most senior subject matter expert (SME) will take the lead on the bridge to focus troubleshooting efforts on service restoration. A Public Information Officer (PIO) will also be assigned to manage communications with affected PSAPs and the Commission. Each affected PSAP will be contacted either by a member of the NOC/SOC staff, the PIO, or their designee.

Troubleshooting will continue until service has been restored. PSAPs and the Commission will continue to receive regular updates as troubleshooting continues. The conference bridge will be maintained until service is restored. Backup systems, such as the MEVO(+) disaster recovery platform, will be utilized to restore a temporary level of service. These changes will be communicated directly to the PSAP.

Given the duration of the event, an after-action report will be prepared to include a root cause analysis (RCA).

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement GEN SCEN 2.				

Any additional documentation can be inserted here

In the proposed design, all legacy network gateways (LNG) would be deployed in a redundant manner. This means the LNGs would be redundant in connectivity to the core nodes, as well as physically redundant. This deployment methodology is designed to mitigate this hypothetical scenario. In the event of a catastrophic hardware failure, the redundant LNG would be prepared to begin processing the calls.

In the proposed scenario, initial steps would involve corroborating the data. Calls would be placed to PSAPs to determine if PSAPs are receiving a lower than normal number of 9-1-1 calls. If PSAPs are receiving normal call volumes, the troubleshooting would focus around the logging processes. If the PSAPs are not receiving normal call volumes, we would begin to look at the ingress trunking from carriers. While there is a single failed LNG that must be restored, the failure of three LNGs simultaneously seems unlikely and would likely indicate trouble higher in the network, such as the OSP network. Once the impaired trunks are identified, the NOC/SOC staff would place a trouble ticket with the representative OSP and coordinate efforts to restore services.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement GEN SCEN 3.				

Any additional documentation can be inserted here

GeoComm's system provides the ability to configure quality and threshold levels to support data integrity as it will be used in public safety applications. Setup would include:

- Flagging certain quality checks as critical so any reports would stop provisioning into the public safety application
- Setting warning level QCs with a threshold to either send a notification that a threshold has been exceeded or stop the provisioning due to a threshold being exceeded
- Setting a change threshold (changes as a percent of the whole dataset or changes as they compare between inserts and removes) that could be set to either send a notification that a threshold has been exceeded or stop the provisioning due to a threshold being exceeded.

This ability keeps the data maintainers updated on their data quality and provides information that may indicate degradation of the data that was unintentional.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement GEN SCEN 4.				

Any additional documentation can be inserted here:

The proposed ESInet is designed to failover between the primary and secondary links. In this scenario, a failure of Link A would indicate that the Regional Call Host (RCH) is continuing to operate on Link B. NOC/SOC technicians will begin diagnosing the trouble on Link A. If the terminating equipment at both ends checks out, a trouble ticket will be placed with the underlying provider of the link.

Given that at 0725 Link B begins to bounce, focus will then be given to the potential for a folded ring scenario. The proposed network is designed to be carrier and route diverse. Both links failing is indicative of a single fault domain, either hardware or route.

By 0900, if the transport issues are not resolved, policy would dictate that escalation should have already began. A bridge should be established, and appropriate technical staff should be engaged. As the RCH has reported a decrease in the number of calls, logging will be queried to determine whether the "lost" calls are being delivered to another answering point or if they are being "lost." If the primary answering point is not receiving the calls, we would look for the policy routing function (PRF) to be delivering the calls to the next asset. Most likely this would be MEVO(+) at the original PSAP or a rollover Region/PSAP. Ensuring that all initiated calls are delivered is the primary focus.

The proposed solution includes a tertiary connection that would be utilized in this scenario to restore service. Typically, this connection would be utilized automatically with no manual intervention from the RCH/PSAP or the NOC/SOC.

PM 1	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement PM 1.				

Any additional documentation can be inserted here:

Project Management Methodology

Relationship management is a key component of Hamilton's project management methodology and Hamilton will allocate appropriate, qualified personnel to fulfill all objectives of the implementation, testing, cutover, provision of, support, performance of, and maintenance for the ESInet, NGCS, and other obligations and commitments as set forth in this RFP.

Hamilton will assign a Project Manager to oversee the implementation and completion of the Acceptance Test Plan (ATP) and the Cutover Plan (CP). The individual assigned as Project Manager will be Peggy Christensen, PMI Project Management Professional (PMP), and will be dedicated to the Commission during the implementation of the project and for a period of one (1) month following the last Regional Call Host (RCH) Go-Live Date to ensure all Services are stable, are in full compliance with the ESInet and NGCS requirements, and meet all SLAs. This individual is certified under the PMI Project Management Professional (PMP) program and is designated as a Key Personnel. A resume for Ms. Christensen can be found in original Appendix 5 – Hamilton Resumes and References.

As mentioned, the solution proposed includes a certified Project Manager with an executive management sponsor to oversee the project goals and objectives. In addition to the Contract Manager, this individual will serve as a primary contact with all contracted staff to ensure the project schedule and all milestones are met. To accomplish this goal, the project manager will apply appropriate Project Management Institute principles that align with the Project Management Body of Knowledge (PMBOK).

Additionally, the Project Manager will report to the designated Commission employee and will be onsite during important project events, such as the installation of the core system. This project manager will communicate with the designated Commission employee and will also serve as a liaison and point of contact for originating service providers (OSP), additional Commission personnel, and stakeholders. This individual will fully coordinate and organize weekly project status calls to review the execution of tasks and activities, focused on the statement of work (SOW). The statement of work will include a responsibility matrix for the project.

Additionally, a written report will be regularly prepared, aligning with the state boards meeting schedule, for the benefit of board members. This will be presented in-person and will provide an update on the status and progress of the project.

Any outstanding tasks or action items identified as key to the success of the project will be coordinated and assigned by the designated Project Manager. This process of high-level management, collaboration, and execution of tasks will result in the successful implementation and management of the proposed ESInet and NGCS as defined in the RFP and resulting contract.

Following contract execution, the Project Manager will coordinate a kick-off meeting with Commission personnel, working together to establish expectations and content ahead of time. Following the completion of the kick-off meeting, the Project Manager will provide a detailed project schedule including project phases, tasks, and milestones with specific starting and completion dates. This project schedule will provide a baseline for the weekly updates provided to the Commission for approval. Please see Appendix 11 – Nebraska Project Plan Template and Appendix 12 – Nebraska Project Lifecycle Template for an example of Hamilton's project schedule and major milestones, with an example start date of October 1, 2020.

The signed contract will serve as the project charter and budget baseline. Project management plans include:

- Work Breakdown Structure (WBS)
- Schedule Baseline
- Change Management
- Communications Management
- Conflict Resolution
- Acceptance Testing
- End of Project Report
- Lessons Learned

Technical documents will include originating service provider (OSP) conversion documents, "as built" drawings, comprehensive test plans, build sheets, policy routing function (PRF) documentation, training materials, project notes, and other ad hoc reports as needed.

Support Structure

Hamilton's maintenance and support operations are transparent, easily accessible, and delivered in the most effective and efficient manner possible. System reliability and maintainability are major components driving the concept and design of the Hamilton NG9-1- 1 system. Furthermore, we recognize the importance of system availability when public safety and life-saving responses depend on calls going through to the PSAP.

Because of our experience in providing critical public safety services for over 50 years, Hamilton has the necessary expertise and capabilities to deliver support to our customers, ranging from full remote support to on-site operational responsibilities. The performance under our current contracts has allowed us to establish and maintain a highly qualified technical staff, comprehensive technical capabilities, and service delivery efficiencies. Hamilton has deep-seeded roots in the telecommunications industry, bringing significant competency in data solutions, including hardware installation and maintenance.

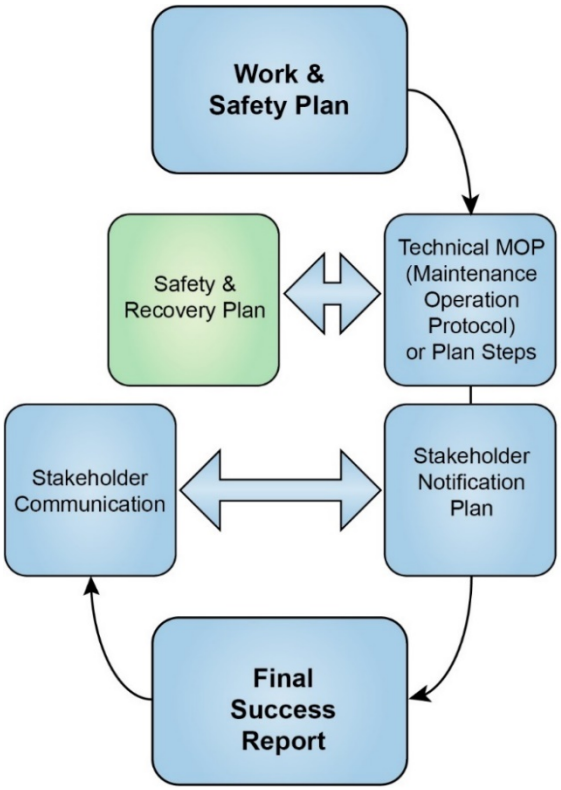
The foundation of Hamilton's Maintenance & Support Operations is based upon the following:

- Preventative maintenance through the implementation of a comprehensive maintenance plan inhibits problems before they occur.
- Resolve issues using industry accepted standards and best practices, including NENA recommended standards.

- Effectively utilize industry experts and staff to execute operational requirements.
- Provide a comprehensive turnkey solution for both network operations and management.

The overall architecture detailed throughout this technical proposal is highly redundant to meet the 99.999% availability requirement. The system proposed includes a state-of-the-art network management and reporting solution to monitor and operationally support the next generation environment. Hamilton is committed to maintaining and managing the entire network and all components as a single system to ensure end-to-end service quality.

Proactive monitoring of the network, data centers, and other systems and facilities is performed as a key component of our overall maintenance plan. Hamilton will follow the Work and Safety Plan (WSP) illustrated below as the process for planning any scheduled maintenance activities.



The WSP is a document that focuses on (1) the planned work, or maintenance, to be performed and (2) a safety plan to be utilized in the event the maintenance work does not go as expected. The WSP also includes a 'rating' scale used to forecast the likelihood of a service impact/disruption due to the maintenance work. The WSP focuses on documenting a primary plan, creating a backup plan, peer review, results verification, and stakeholder notification.

Hamilton will work collaboratively with the Commission when considering, scheduling, and performing maintenance to discuss risk, impact, and the reasons for such maintenance. Additionally, Hamilton will present and discuss recommendations for applying the maintenance patches and upgrades in a manner that best meets the requirements and the best interest of the state. This ensures the WSP work is scheduled in a pre-defined maintenance window with prior notification provided to designated points of contact. Most commonly, maintenance is performed remotely, leveraging the redundancy of the systems to ensure no impact to the state's services. When on-site maintenance is needed, Hamilton will provide the necessary trained and qualified technicians that will commence on-site repair activities for system malfunctions within the time frames mutually agreed upon by Hamilton and the Commission.

To accomplish this goal, the Maintenance Manager and their key staff will operate out of the main Network Operation Center/Security Operations Center (NOC/SOC) located in Fort Wayne, Indiana. This NOC/SOC also houses the help desk and test lab which cumulatively provides monitoring, security, and maintenance services throughout the duration of the contract and delivered with, and managed, according to applicable service level agreements (SLA). The NOC/SOC specializes in 9-1-1 service management and serves as a single point of contact for all PSAPs, interconnecting parties, and the Commission. Maintenance and support services located at the same facility ensure the benefit of reduced reaction time and improved communication as the help desk and NOC/SOC personnel will coordinate efforts and response actions.

This intentional design of the monitoring capabilities provides for aggregated results, enabling Hamilton's trained personnel to monitor multiple components of the solution simultaneously, reviewing, making recommendations, and performing actions so that the systems and customer solutions are functioning at optimum efficiency.

The proposed solution is architected to utilize both redundancy and geographic diversity to ensure a fully redundant solution. Each of the two geographically diverse core routing nodes consist of redundant hardware and software for all critical elements. Leveraging both the physical redundancy within each core routing node and the geographically diverse nodes ensures that any component failure does not result in an outage of the function it performs. Rather, service is rerouted around the failed component to other active resources. Physical and geographic redundancy guarantees that a component failure will allow full capacity at the other node to ensure system uptime remains at 99.999%.

Planned maintenance events are managed in a similar fashion. Utilizing redundant components and geographically diverse nodes, a single node or component can be temporarily decommissioned for maintenance while maintaining full availability of call routing and call delivery service. This allows component/element maintenance that does not impact the overall service.

Regarding new standards and updates to the working system, Hamilton tests extensively in its lab environment located in Ft. Wayne, Indiana. In addition to utilizing the test lab, Hamilton also uses a comprehensive test plan for upgrade and maintenance projects. Hardware and software maintenance are coordinated across several work groups, with cross checks for work quality. The NOC/SOC tracks service availability and maintenance needs.

When planning and executing maintenance and configuration updates, Hamilton adheres to a structured approach. Maintenance events include the WSP created to provide notification and transparency to 9-1-1 system stakeholders. The focus of the WSP is on documenting a primary plan, creating a backup plan, peer review, results verification, and stakeholder identification.

When maintenance work is necessary, Hamilton creates a comprehensive document describing specifically which work needs to be completed and a step-by-step guide on the work that will be completed. Once the maintenance work is complete, a detail report is provided including the corrective and/or preventative actions taken. These reports will include events by date and time range and specific events.

By utilizing the MEVO(+) disaster recovery platform during scheduled maintenance activities at the PSAP, PSAPs can maintain full functionality allowing dispatchers to “operate as normal,” while utilizing a backup system. The use of this platform adds additional assurance of no downtime or negative impacts to call-delivery and call-processing operations.

While MEVO(+) is a components of Hamilton’s continuity and disaster recovery system, both solutions are designed to ensure delivery of calls and automatic location information (ALI) to the Regional Call Host (RCH), or PSAP, in the event of an impairment of the ESInet or primary 9-1-1 call handling solution. They are also ideal solutions during scheduled software releases to maintain continuity of operations.

It is imperative that maintenance of the Hamilton NG 9-1-1 solution is done with no scheduled downtime, nor should it trigger an SLA event. Overall, all maintenance and updates are well planned, organized, and documented in a manner that does not impact 9-1-1 operations.

Additionally, Hamilton will utilize a full portfolio of monitoring tools including NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and logging subsystems. Along with active alarming, these monitoring tools are employed to identify potential problems before they occur. The NOC/SOC utilizes monitoring systems to log and alarm all facets of 9-1-1 services in near real time. This includes bandwidth usage, memory usage, CPU usage, and services availability. This includes all Hamilton devices in the core and PSAP.

The use of these monitoring platforms provides dashboards to provide comprehensive visibility and monitoring of the present state of the network, to include any loss in redundancy. As a result of this extensive visibility, abnormal traffic will immediately be detected and customized alarms and threshold settings can be established, providing instant alerts and notifications via visual display, text, or email. These platforms are utilized to provide authorized stakeholders with access to a network status dashboard allowing the proactive monitoring of systems, statistics and visualizations in near real time. Additionally, alerts and alarms will facilitate the involvement of NOC/SOC personnel in the event service escalation becomes necessary.

Overall, the NOC/SOC and helpdesk will be staffed with trained personnel that will work collaboratively to provide monitoring, maintenance, and support services for the proposed NG 9-1-1 solution. The NOC/SOC will monitor performance issues, faults, and failures and will have the capabilities for re-routing, as well as additional types of recovery and management functions. Where actionable issues are identified, the NOC/SOC staff will provide notification to all designated recipients and generate trouble tickets.

Communications Plan

This Communications Management Plan will serve as the framework for communications throughout the duration of the project to include daily, weekly, and monthly interaction during the migration. This section will include a high-level summary of the communications plan and a preview to this section of our response. It will also identify the responsible party who will manage all forms of communication.

Communication Type	Description	Frequency	Format	Participants/ Distribution	Deliverable	Owner

Kickoff Meeting	Initial project meeting with Customer. Represents the transition from Executive or Sales team to Project team. Goal is to review contract deliverables and initial project plan. Will also work through additional engineering details as needed. This is the first opportunity for Project team to engage customer with questions.	Once	Face to Face	Executive Sponsor(s), Sales Team Project Manager(s), Customer, Customer's Consultant	Initial Project Plan	Executive Sponsor
Weekly Status Report	Project Manager delivers weekly update to Customer. Call is also used to address changes to project plan. Market Manager becomes engaged as a liaison between Customer and PSAPs.	Weekly / Project Duration	Conference Call	Project Manager Sales / Market Manager, Engineering, Provisioning, Customer, Customer's Consultant	Status Report	Project Manager
Weekly Project Team Meeting	Internal meeting to discuss action items and project plan with project team.	Weekly / Project Duration	Conference Call	Project Manager Sales / Market Manager, Engineering, Provisioning	Action Items List from Project Team	Project Manager
Project Monthly Review	A Monthly meeting held to review ongoing projects. The PMO leads this meeting and seeks a report from each Project Manager. The goal is for the Executive Sponsor to gain a current	Monthly	Conference Call	Project Management Officer, Project Manager(s), Exec. Sponsor / Market Manager(s)	PMO Report to Exec. Management	Project Management Officer

	project status, a list of gating items and a list of areas of change to scope or plan. That information will then be used to either redirect internal resources or address with customer for potential change order.					
Project Gate Review	Part of bi-weekly project review.	Ad Hoc	Conference Call	Project Management Officer, Project Manager(s), Exec. Sponsor / Market Manager(s)	PMO Report to Exec. Management	Project Management Officer

Specific to weekly reports, Hamilton understands the importance of regular project communications and will facilitate weekly project calls, and document said calls with meeting minutes distributed within 24 hours of project calls. In addition, Hamilton will distribute weekly written progress reports on an agreed-upon schedule.

Hamilton's Weekly Progress Reports will contain details regarding the following tasks: data gathering, staging and lab testing, and installation progress at each site.

More specifically, Hamilton's progress reports typically contain the following components:

- A list of tasks/activities accomplished, and Deliverables completed, including progress on the Acceptance Test Plan and/or Cutover Plan since the last Weekly Progress Report;
- A list of risks and outstanding Issues identified by the Commission and/or Hamilton that remain to be resolved; and
- Any other items as set forth in the Acceptance Test Plan and/or Cutover Plan and any other items as agreed between the Commission and Hamilton.

As detailed above, Weekly Progress Reports will be thorough and any delays, issues and risks related to the Commission, Hamilton, originating networks, County 9-1-1 Authorities, and/or other third parties will be included

Project Plan

Hamilton has included a high-level overview of the project plan and timeline depicting the entire project calculated from the example start date of October 1, 2020. The regional implementation order within the sample project plan is based upon the NGCS Milestones as included in the Cost Proposal document. However, Hamilton is willing to work in any implementation sequence the state specifies and Hamilton will work collaboratively with the Commission to create a more refined project plan during the contract process.

Hamilton's sample project plan is included as Appendix 11 – Nebraska Project Plan Template.

Implementation Schedule

Hamilton will collaborate with the Commission to create a phased implementation plan, creating a solution that conforms to NENA-INF-016.2-2018, Emergency Services IP Network Design Information Document (ESIND).

The solution proposed includes all next generation core services (NGCS) functional elements (FE) to support an end state NENA i3 functional ESInet, as well as the FEs required to functionalize the ESInet during the implementation and transition phases.

These functional elements include the border control function (BCF), emergency services routing proxy (ESRP), legacy network gateway (LNG), legacy PSAP gateway (LPG), legacy selective router gateway (LSRG), location validation function (LVF), policy routing function (PRF), and logging service.

Our implementation plans identify where the NG 9-1-1 FEs are located, how they are configured, and provides documentation including "as-built" information that describes their operation and function within the NG 9-1-1 system. Hamilton shall build and test the ESInet in advance of, or in parallel with, the build and test of next generation core services (NGCS) nodes, submitting plan tasks for the integration and joint testing.

NGCS nodes will be redundant installations within Nebraska to maintain the highest levels of system uptime. The Nebraska Data Center (NDC) and Hamilton Data Centers will be utilized and will also function as the two primary points of interconnection (POI) with originating service providers (OSP) and network providers. Each legacy telephone company will establish trunks to NDC and the Hamilton Data Center. Also, each wireless and VoIP provider will be asked to establish IP based NNIs at each data center. Additional POI's have been anticipated in each LATA for OSP 9-1-1 trunking termination, and an initiative to modernize some OSPs to session initiation protocol (SIP) interconnections, are built into the proposed response.

FEs in the call flow are redundant and deployed in an active / active configuration. This means each element located in either data center can process and terminate calls in parallel or stand alone at each NGCS site.

The proposed solution will require carriers to establish at least two points of interconnection with enough trunks to maintain normal service delivery in the event of trunk or link issues at one of the data centers.

The solution employs redundant legacy network gateways (LNG) (SS7, PRI, or CAMA), session border controllers (SBC) for secure ingress SIP connections, and legacy PSAP gateways (LPG) on the egress of the ESInet.

Additionally, the solution provides a third route to the NGCS nodes via Communications Security, Reliability and Interoperability Council (CSRIC) best practices of providing an 800 number for failover routing. This functionality allows the NGCS nodes to identify the calling party number and process it as automatic number information (ANI).

As Hamilton approaches the end state NENA i3 ESInet/NGCS, Hamilton will provide "as-built" drawings, architectural diagrams, design documents, rack layouts, wiring diagrams, and configuration files in electronic form.

A detailed sample implementation timeline for all aspects of the proposed solution can be found in Appendix 11 – Nebraska Project Plan Template.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement PM 2.				

Any additional documentation can be inserted here:

Hamilton will provide extensive post-implementation client management services, which includes a dedicated Post-Implementation Client Manager. It is Hamilton's responsibility, specifically the Post-Implementation Client Manager, to ensure collaboration is maintained and planning occurs for what should happen after the project has been successfully delivered. Hamilton will continue to work with the State to ensure that needs are identified and continue to be addressed in a professional and timely manner.

Beside working directly with the designated Post-Implementation Client Manager, client management reports, executive briefings, and ad hoc support request can also be directed to Hamilton's 24x7x365 NOC/SOC, which can be reached by email, phone, or through the dedicated portal made available specifically for the project. In addition, the Communications Plan, referenced above in Hamilton's response to requirement PM 1, will remain in effect post-

deployment and will be managed specifically by the Post-Implementation Client Manager.

Through Hamilton's significant, and diverse, history of managing government contracts, we have provided the necessary support to provide superior account management services, which we feel is a distinguishing characteristic of Hamilton. This is proven through Hamilton's track record with maintaining government contracts and receiving subsequent renewals. Hamilton provides a unique and personalized customer service experience and we actively seek feedback to discover what we are doing well and what we may need to improve. Regardless of the situation, Hamilton is committed to working collaboratively with the State to find a realistic solution that will satisfy the State's needs, while always providing a suburb service at an exceptional value.

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).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement TRN 1.				

Any additional documentation can be inserted here:

Hamilton will provide comprehensive training to designated Commission representatives responsible for varying layers of network/system monitoring and system maintenance. This will include training prior to the first Regional Call Host (RCH) transitioned to the network as specified through Hamilton's Project Plan.

Hamilton has experienced training resources that can deliver training at the state, regional, and local level throughout the state of Nebraska as needed. These resources have many years of experience providing training and will continue to provide ongoing training to ensure Regional Call Hosts (RCH) and Commission representatives are fully prepared and equipped. Trainees will receive the necessary knowledge empowering them to manage user interfaces, access portals, and run reports. In addition, the State and its users will gain a clear understanding of the maintenance and provisioning of the network, as well as the ability to understand the maintenance report.

Hamilton's training program includes a variety of topics specific to system implementation and ongoing operation and maintenance and will include the following:

User-Configurable Elements

The policy routing function (PRF) is an integral part of the NGCS system and the component that enables 99.999% availability. The PRF provides alternate routing procedures for call routing in the event of failures in the call flow and the PRF can be unique to each PSAP. The PRF follows a prioritized decision tree after routing to determine where to ultimately deliver the emergency call and Hamilton will work collaboratively with the Commission and PSAPs to create customized PRFs.

Hamilton will also provide training on user access to the PRF and how changes can be made. Today, user access to the PRF can occur via two methods which include (1) contacting the network operations center/security operations center (NOC/SOC) and utilizing the change management process and (2) to invoke policy change through the use of the Optimal Service Button on the MEVO(+) disaster recovery and backup platform. This service enables a credentialed user to invoke a predetermined policy. Hamilton will provide all relevant PRF policy management training to PSAP and Nebraska stakeholders as required by the Contract.

NOC/SOC Procedures

Extensive training specific to NOC/SOC procedures is included within Hamilton's training curriculum. This training includes train-the-trainer, administrator, and technical training course that have been implemented in other statewide deployments. Hamilton delivers on-site training specific to Nebraska's NOC/SOC functions and copies of all training materials will be provided for review at least 30 days prior to the commencement of training. Documentation is provided in a variety of formats and supporting materials can be accessed via the executive dashboard (website). Hamilton will provide an executive dashboard via the NE911.net website. This portal provides continuous training materials and support to Regional Call Hosts (RCH), the Commission, etc. and will be an ongoing resource for these entities to accommodate staff changes and future training needs. Hamilton also offers a number of training videos, which serve as an additional supplementary training source to provide information specific to NOC/SOC procedures.

Escalations

Hamilton provides a 24x7x365 network operation center/security operation center (NOC/SOC) that can rapidly triage and handle the reports of network incidents. Specifically, Hamilton's ticketing platform, TeamSupport, allows support requests to be manually entered via the web interface and/or auto generated by maintenance tools. Once received, notifications are distributed to the appropriate distribution list based on requirements and tickets are categorized into three priority levels by NOC/SOC staff. Hamilton will provide training to the Commission on its incident management system, which will include all processes and procedures for incident reporting and the utilization of ticketing tools.

Trouble Reporting

Hamilton provides a 24x7x365 network operation center/security operation center (NOC/SOC) that can rapidly triage and handle the reports of network incidents. Specifically, Hamilton's ticketing platform, TeamSupport, allows support requests to be manually entered via the web interface and/or auto generated by maintenance tools. Once received, notifications are distributed to the appropriate distribution list based on requirements and tickets are categorized into three priority levels by NOC/SOC staff. Hamilton will provide training to the Commission and RCHs on its incident management system, which will include all processes and procedures for incident reporting and the utilization of ticketing tools.

Help Desk Portal

Like NOC/SOC procedures, training on the help desk portal is provided through the designated training module on NE911.net. This specific training is provided in a variety of methods, including classroom training with take-home handouts and user guides, live videos, and refresher trainings. Hamilton's help desk operates as a function within the Hamilton NOC/SOC and Hamilton has designated staff who receive specialized training in product support, in addition to their NOC/SOC duties. Hamilton provides a number of additional supplementary training and "help resources" that are made available through the project portal (e.g. videos, whitepapers, etc.) and Hamilton will provide training on how to access these resources, in addition to the help desk portal.

Executive Dashboard

As explained earlier in the proposal, Hamilton will provide an executive dashboard via the NE911.net website. This site will provide the Commission and the region's PSAPs with access to the content required and near real-time visibility into the facilities and elements that compromise the ESInet. As a component of Hamilton's comprehensive training, instruction will be provided on this web-based executive dashboard.

Service Monitoring Tools

911 Logix is Hamilton's comprehensive logging and reporting system and is an advanced reporting tool that aggregates source data and allows for visualization, reporting, and trending of ESInet content in a NG 9-1-1 network. This tool is also highly customizable and provides a means for providing service monitoring tools for the state's NG 9-1-1 stakeholders. While Hamilton provides standard reports, Management Information System (MIS) tools, and performance metrics to RCHs and the Commission monthly or upon request, Hamilton will work with designated system administrators to determine access credentials and the requirements for password formats and security levels. 911 Logix and all dashboards and visualizations are set up with a hierarchical method so that access to data is controlled by the system administrator. Hamilton works with administrators and users to ensure their ability to access and utilize service monitoring tools.

In addition to the training topics mentioned above, Hamilton will develop additional training modules and classes to be made available as the Nebraska ESInet evolves throughout the term of the contract. Within this response, Hamilton has included a sample Trainee Checklist specific to the state of Nebraska. This checklist includes training on topics such as NE911.net, Toolkit, 911 Logix, etc. As Hamilton works collaboratively with the State to determine a training plan specific to the State's solution and needs, this checklist would be adjusted accordingly. The overall goal of including a sample checklist within this

response is to show that Hamilton provides a means for trainees to track their successful completion of training and to further emphasize the importance of adequate training and its inclusion in Hamilton's proposed solution. To view the sample checklist, please see Appendix 13 – Trainee Checklist – State of Nebraska.

Hamilton has highly experienced trainers on staff, many with extensive dispatch experience. The training syllabus is comprehensive, and covers all user interfaces, processes, escalation, and general industry knowledge. Training for the proposed solution will include comprehensive training and ongoing support in compliance with all the requirements outlined above.

While more information is provided below regarding training logistics, Hamilton's training consists of classroom style training with take home handouts and user guides. Class training includes live video and two-way interaction throughout the session. Refresher and on-demand training are available by a web menu of resources available at any time, including Q&A worksheets, video modules and other materials. All training will be backed and further reinforced by regional meetings, as well as statewide training sessions covering beginner and advanced topics.

Hamilton operates multiple statewide networks and has extensive experience in coordinating training materials and strategies with 9-1-1 state program offices. This collaboration and partnership results in an exceptional state 9-1-1 program. Hamilton is fully confident that it can comply with this requirement and commits to providing extraordinary training to the Commission and RCHs.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement TRN 2.				

Any additional documentation can be inserted here:

Training Logistics & Curriculum

Hamilton understands that for Nebraska to have a successful implementation of their new NG 9-1-1 emergency communications system, effective training for the right people, at the right time is crucial. Training should be a well-planned activity integrated into the overall project plan to design, equip, install, operate, monitor, maintain and support the system and Hamilton acknowledges the importance of a high-quality training plan in the overall success of the system. Hamilton is extremely experienced in providing varying levels of technical training both to internal employees and external customers. Investing in Hamilton staff, through training and opportunities for professional growth, is one of Hamilton's core competencies. For example, in 2019 alone, Hamilton Relay successfully provided highly complex training to over 1,000 staff members that provide Captioning and Traditional Relay services at Hamilton Relay Call Centers around the United States. Additionally, Hamilton provided training to approximately 500 external business key phone systems customers within the last year. Providing training is an area of expertise for Hamilton and we look forward to applying this knowledge and experience in our training with Commission and PSAP employees.

Hamilton plans to deliver its training course in multiple areas throughout the state of Nebraska to accommodate the approved development schedule. Extensive collaboration will occur between Hamilton and the Commission as the Commission will help coordinate all classes and will determine and secure the training locations based on the specific deployment schedule. Hamilton also realizes that training class sizes for each session should be moderately sized to allow for interactive learning and ample opportunities to ask questions and facilitate dialogue regarding the training being delivered. Hamilton schedules training classes at the PSAP (or the PSAP's designated training facility), during normal working hours (generally 8 am – 6 pm), and class sizes typically only include eight individuals per trainer depending on space availability.

Hamilton is well-versed in making its training highly accessible and training will be made available in a variety of modalities, such as web-based training, instructor-led training, and electronic and paper documentation. In addition,

Hamilton can provide multilingual training instructors if needed and will work with the Commission to adequately address all training logistics.

Proposed Training Plans

This proposal includes a comprehensive training program, consisting of field-proven train-the-trainer, administrator, and technical training courses that have been implemented in other statewide deployments. Hamilton has staff trainers with dispatch experience and training is comprehensive for all user-configurable elements, NOC/SOC procedures, escalations, trouble reporting, as well as other topics listed within requirement TRN 1. Experience operating multiple statewide networks and coordinating training materials and strategies with state program offices will be leveraged in order to build a strong state program with the PSAPs.

Many of the systems proposed are newer versions of the existing systems as requested or listed as preferred by Nebraska. Hamilton will leverage its experience in creating similar training and support materials for other clients and will customize content based on the needs of Nebraska.

Hamilton will deliver on-site training specific to specialized Nebraska functions and copies of all training materials will be provided for review at least 30 days prior to the commencement of training. Also, prior to the start of training, Hamilton will provide a training plan that includes any applicable training requirements following the implementation and acceptance of the proposed solution. The documentation to be provided will include training materials for both administrators and end users, along with build sheets, user manuals, diagrams, and operations documents. Within this response, Hamilton has included an example training plan specific to its MEVO(+) disaster recovery platform. This training plan maps out a three-hour training session including training expectations and content to be included within the session. This training plan for MEVO(+) serves as a single example of Hamilton's exhaustive training materials and the type of organization and format the State can expect from Hamilton specific to training. Please see Appendix 14 – Sample MEVO(+) Training Outline.

In addition, Hamilton offers online training videos specific to the Legacy Database (LDB) Manager website. These videos are accessible through the website and cover a variety of topics geared towards users of the LDB. LDB users will learn how to lookup devices, add/modify/delete records, fix discrepancies, retry service order input (SOI) records, and resolve "No Record Found" responses, among other things. To supplement the training videos, Hamilton also offers documentation in the form of a User Interface Guide and a Quick Reference Guide. These documents outline the acceptable file formats, outgoing reports, and workflows for the LDB.

Training specific to the ECRF and LVF will be provided remotely. It will focus on the functions and architecture of the software. In addition, training will provide an overview of the ECRF and LVF systems within the overall NG 9-1-1 system. The provisioning process and maintenance of the system will also be covered. Key data quality processes will be included in the course along with descriptions of interfaces. The State will be responsible for determining the appropriate staff to participate in the training sessions. Typically, IT or administrative professionals and a lead GIS technical representative attend the training. As the training will be provided remotely, the State may determine the appropriate number of attendees. Training is intended for ECRF/LVF system administrators and individual users.

Training Materials

Within this response, Hamilton has included sample training materials for 911 Logix. These training materials can be found in Appendix 15 – Hamilton Training Materials. In addition, Hamilton has provided the following URLs to view three 911 Logix training videos developed as a training tool for the state of Alabama at the onset of that state project. These videos accurately depict some of the data and functions that can be made available to Nebraska. Please note that these privately hosted videos will be made available, via the following URLs, for 90 days:

- Logix Training – Part I – Access: rb.gy/vm76tq
- Logix Training – Part II – Buttons: rb.gy/zbpmlq
- Logix Training – Part III – Reports: rb.gy/x7ga6i

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SRAR 1.				

Any additional documentation can be inserted here:

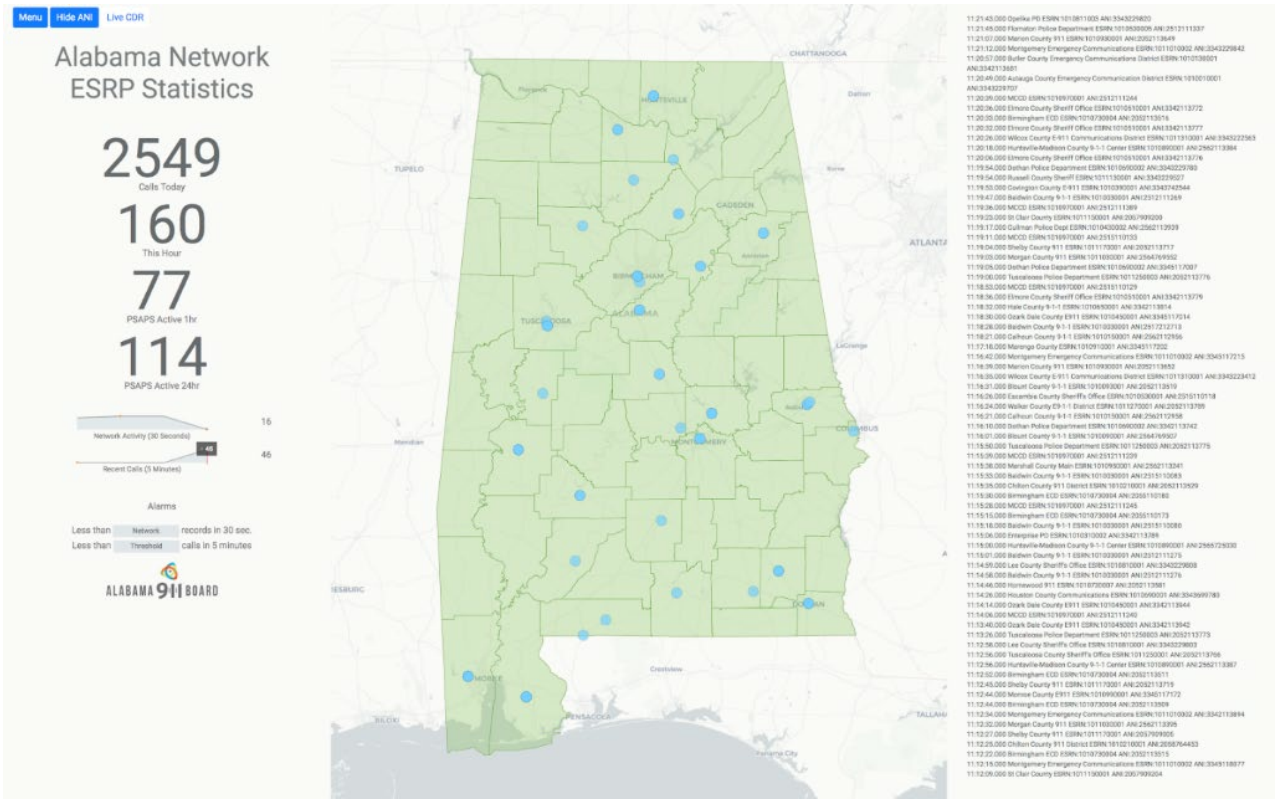
Replacements, Upgrades, & Malfunctions

The proposed service is an all-inclusive "9-1-1 as a service" model. Therefore, Hamilton will be responsible for all costs associated with all hardware, software, and applicable services replacements whether the cause is due to end-of life by the manufacturer, a product is defective or unserviceable due to failure or malfunction, or an upgrade is deemed necessary to maintain continuity of operations.

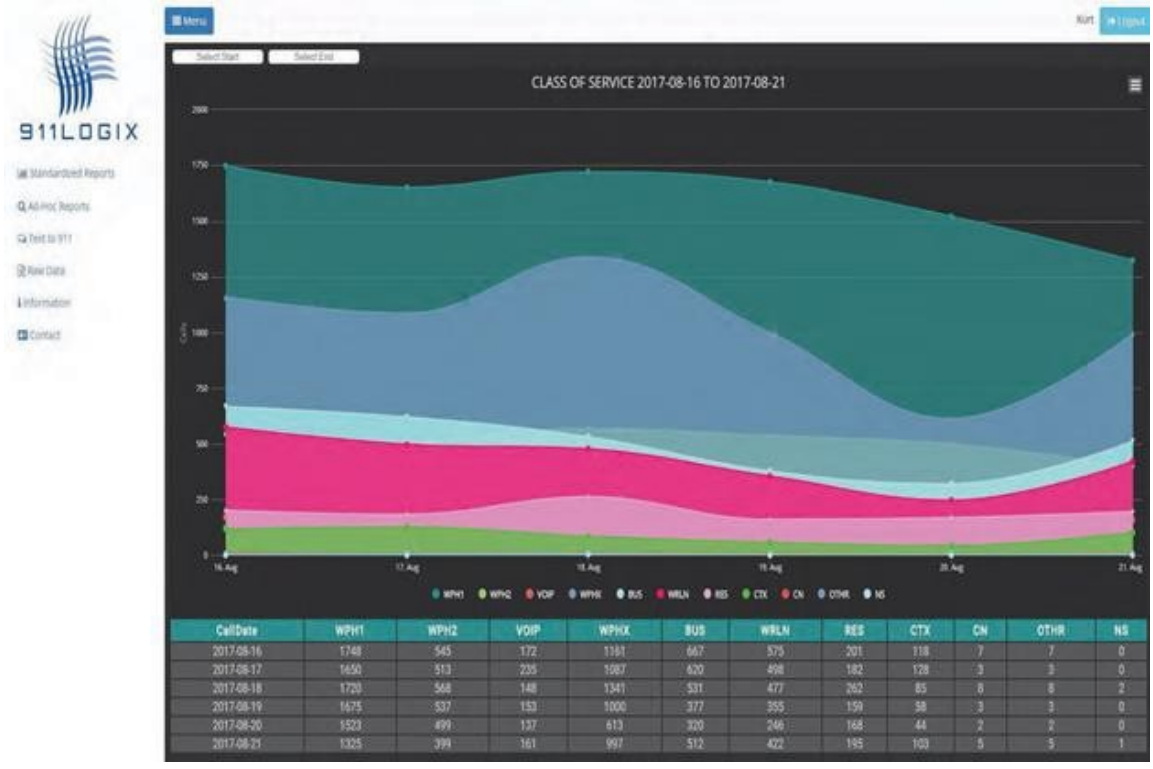
24x7x365 Maintenance Support

The proposed solution provides a 24x7x365 network operations center/security operations center (NOC/SOC) specializing specifically in 9-1-1 network management. This "always available" NOC/SOC can be reached at any time via email, telephone, or through a web portal. This NOC/SOC utilizes a comprehensive toolset of monitoring applications, including NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and logging subsystems.

Additionally, Hamilton will routinely complete audits of PSAPs and transport circuits, verifying records and maintaining physical and logical patch diversity relationships. The platforms listed earlier (i.e. NAGIOS, etc.) provide dashboards to provide comprehensive visibility and monitoring of the present state of the network, to include any loss in redundancy. As a result of this extensive visibility, abnormal traffic will immediately be detected and customized alarms and threshold settings can be established, providing instant alerts and notifications via visual display, text, or email. These platforms can be utilized to provide the Commission with access to a network status dashboard allowing the proactive monitoring of systems, statistics and visualizations in near real time. Images are provided and explained below of Hamilton's 911 Logix monitoring application.



This image depicts a statewide activity view for call routing in the state of Alabama and provides an example for the state of Nebraska. The dashboard can be customized to include call data, trends, and threshold alarming. The system also provides the ability to collect and visualize NENA i3 logs from different systems such as next generation core services (NGCS), automatic location information (ALI), text-for-9-1-1, and CPE.



CallDate	WPH1	WPH2	VOIP	WPHX	BUS	WRLN	RES	CTX	CN	OTHR	NS
2017-08-16	1748	545	172	1161	667	575	201	118	7	7	0
2017-08-17	1650	513	235	1087	620	498	182	128	3	3	0
2017-08-18	1720	568	148	1341	531	477	262	85	8	8	2
2017-08-19	1675	537	153	1000	377	355	159	58	3	3	0
2017-08-20	1523	499	137	613	320	246	168	44	2	2	0
2017-08-21	1325	399	161	997	512	422	195	103	5	5	1

Maintenance & Notification Process

In conjunction with its 9-1-1 system stakeholders, Hamilton has created industry-leading maintenance procedures and work guidelines. Hamilton's proposed solution for notification will be customized to meet FCC regulations and the operating needs of the state, county, and federal stakeholders. As a 9-1-1 Service Provider in other states, we are accustomed to providing maintenance notices to all stakeholders when critical maintenance is being performed.

The process for planning any scheduled maintenance activities is as follows and is illustrated in the below. The overall work and safety plan (WSP) was created to provide notification and transparency to 9-1-1 system stakeholders. The WSP focuses on documenting a primary plan, creating a backup plan, peer review, results verification, and stakeholder identification. In the event that maintenance work is needed, Hamilton creates a comprehensive document describing what work needs to be completed and a step-by-step guide on the work that will be completed.

Once the plan has been created, notification is provided to all stakeholders. Additionally, WSP work is scheduled in a pre-defined maintenance window with prior notification required to designated points of contact.

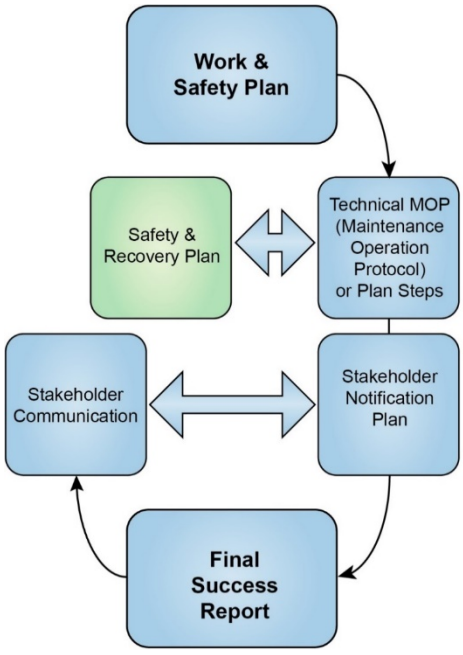
The technical work is described, and expected maintenance results are defined, in the Maintenance Operation and Protocol (MOP) document. Once maintenance has been completed, a final success report is issued, and all stakeholders listed within the MOP are notified with results.

Also, within the MOP document is a safety and recovery plan if maintenance work does not go as anticipated. If this were to occur, Hamilton will return to the service restoration plan contained in the WSP. We have found this process to be extremely successful in creating an environment of consistent quality results.

Problem Resolution & Change Management Processes

Hamilton's problem resolution and change management processes, as well as the supporting systems, adhere to industry best practices, such as the five Information Technology Infrastructure Library (ITIL) stages of continuous service improvement. This is part of Hamilton's organizational culture.

Hamilton's proposed solution includes the following change management processes:



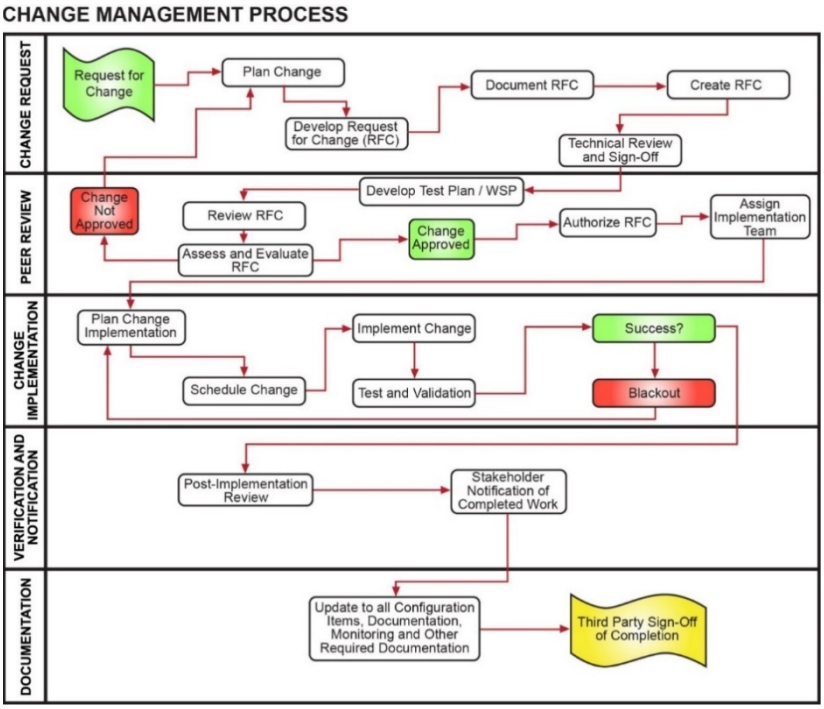
I. Planned Change Management

Effective change management is of vital importance to emergency communications systems. If not managed correctly, changes introduce unnecessary risk. We manage this risk by following processes to help us analyze and plan the change, then implement the change in a controlled and considered manner. The complexity and rigor of the change management process depends on the magnitude and impact of the change. During the planning phase of the project, a Change Register Report (CRR) will be created specifically for the Nebraska NG 9-1-1 project and submitted for approval by the designated Nebraska NG 9-1-1 Project Manager.

All system changes require technicians to create a Change Management Process (CMP). The primary goal of the CMP is to require technical staff to create a plan, get technical sign off, document work, verify results, advise stakeholders of planned work and notify stakeholders upon completion.

After action reports (AAR) are a component of the CMP and are generated following all system changes, whether there was a negative impact to system performance or not. This allows for documentation of all pertinent information generated during system change processes.

All CMPs, including AARs, are made available to the customer. Please see the change management process in the figure below.



II. Unplanned Change Management

Unplanned change events are typically emergency maintenance events. The same change control and maintenance notification processes utilized during planned events are also required as part of an unplanned event.

Notification to customers and other parties is required before any unplanned maintenance event. Notifications provide a summation of the work to be performed, along with an advisory as to the likeliness of the event causing an interruption in normal operations.

Work processes during an unplanned event are also required to follow similar procedures to a planned event. For example, a Maintenance Operation and Protocol (MOP) document must be created and approved by appropriate management prior to the completion of work.

The goal during an unplanned event is to ensure as much planning and communication is completed to ensure seamless call delivery.

III. Change Requests & Updates

Hamilton's solution for reporting and data collection, 911 Logix, will provide enterprise-wide reporting specific to PSAPs and is customizable, providing an efficient and transparent way to monitor, report, and analyze data. 911 Logix will provide the means for the Commission to request changes and receive updates on progress.

If awarded the contract, the Commission's customized web portal will provide a real-time view of the network, including the drill-down capability to a specific device. This portal will allow the Nebraska NG 9-1-1 network and PSAPs to cooperatively view, track, and manage the solution.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement SRP 1.				

Any additional documentation can be inserted here:

Frequency of Scheduled Software Releases

Next generation core services (NGCS) functional and supporting elements are developed under the Agile Development strategy. This development process involves cycles, called sprints, used to develop and code features, or functions, that are eventually collapsed into viable releases.

Each functional element, depending on its maturity, will have its own specific sprint and release lifecycle. These cycles include new features from the product roadmap and bug fixes as they are needed. It is important to note that bug fixes take the highest priority over other work. Currently, the sprint and life cycle frequency are determinant on demand. For example, the recently emerged second generation ingress emergency service routing proxy (INESRP) product has a frequent sprint/release cycle of every seven days. However, not every release makes it to a release candidate and some work is completed in incremental steps working toward a viable release. For example, there have been several viable releases of INESRP as of this writing in 2020. However, the cycle will slow as testing is completed. In contrast, mature functional elements, like the ingress border control function (INBCF), have the same targeted sprint cycle of seven days, but much longer release cycles. For example, the INBCF has a only one or two release cycles, during the same period as compared to the INESRP.

Though the cycles are dynamic and based on business demand, from an informational perspective, there is not an i3 functional element that does not have an active sprint/release cycle for the foreseeable future. The NGCS functional elements are in constant refinement mode through at minimum 2022 in order to cover the needs of new features and functions for emerging projects, or those roadmap items that are under contract. The products will continue to adapt to emerging standards and there is a constant strive to better hone the product(s) with incremental fixes when needed.

Like Hamilton's development and scheduled release processes, GeoComm's development discipline employs agile techniques and aligns with SAFe methodologies. Each of GeoComm's development teams plan and develop in 12-week increments. The typical feature release plan is on an annual cycle, with service pack releases possible on a 12-week basis as needed. In addition, hot fixes (urgent defect resolutions) can be addressed immediately within a current or upcoming sprint which cover a 2-week period.

NGCS Roadmap 2020-2021

Next Generation Core Services (NGCS) / Ingress Emergency Services Routing Proxy (INERSP)

1. Full Administrative/Agency Access to Policy Routing Function (PRF) Rules and Agency Settings: This is the necessary application protocol interface (API) and portal support for an agency to self-create, manipulate and affect change around the call processing rules used to deliver calls to their i3 queues. This function and application provide the ability to securely and safely use policy routing function (PRF) at the network level for those with assigned privileges. Single sign on (SSO) and multi-factor authentication (MFA) are supported for any agency-oriented portal. It is important to note that the portal itself may come from a partnership with a third-party vendor (e.g. using the NGCS provided APIs).

2. Dynamic Queue Registration: Support for DeQueue Registration by ReST, SOAP and SIP REGISTER. This will allow a supporting CHE to dynamically create, and register to, for call delivery. This can be used when the agency has access to policy routing rules (PRR) needed to direct calls to any dynamically created queue.

3. History-Info Support: Full support for History-Info "cause" reasoning, within i3 standards. This function will allow CHE to recognize and identify the purpose of a call diversion or re-route. This can be used by skills, priority and other queueing mechanisms to refine automatic call distributor (ACD) and call handling strategies.

Next Generation Core Services (NGCS) / Ingress Border Control Function (INBCF)

4. Network-based Blind/Warm Transfer: Currently, the supported Conference Focus supports a full attended transfer/conference function at the NGCS/network level. This has been sufficient as the need to create dial-plan wide conferences has been the focus of previous generation networks and the rudimentary transfer gaps filled by CHE that provided the needed direct dial and warm transfer functions. The CHE handled the simpler needs, where large conference solutions weren't needed within the agency.

   As the CHE and networks evolve to multimedia, it is becoming more important that the network supports the full transfer functions previously provided by call handling. This new function will transform the provided Conference Focus to support functions that can be offered seamlessly and consistently for all agencies across the network providing similar blind and/or warm transfer functions as an answer to an emerging need at the network level.

   The current conference focus is based on an intelligent compatible version of i3's "Answer all calls at Bridge" where the use of RFC-4975(Section 5.5) REFER can be used to quickly build a conference of the caller, the original call and as many additional parties as needed and supported at the NGCS level for the project. Please note, this is truly scalable to the thousands. The new function will use any available standard SIP or IMS mechanisms, and Hamilton will work with NENA to get this and/or specific i3 function to allow emerging multimedia call handling to support this as valuable in future upgrades and deployments.

5. Multimedia and Media Independent Conference: The ability for seamlessly conferencing multiple media(s) within the same call, using third party call control to puppet media resources and support for independent media servers, allows for best-of-breed selection of media processing systems. On the surface, this may not seem significant. However, this is extremely important when factoring in the future of media processing (for example, voice transcription and artificial intelligence (AI) based situational awareness). The NGCS model where media processing is a function consumed by the third-party-call control mechanisms within the i3 function elements affords for flexibility and customization at the micro-function level for future proof and innovative solutions. The INBCF solution is certified with multiple SIP Meetme and Dialogic's XMS Media Resource Functions for reliable immediate function. But, the "open" model allows for integration of other applications related to conference, dial-tone multi-frequency signaling (DTMF) capture, and/or custom interactive multimedia retrieval (IMR) type applications.

Next Generation Core Services (NGCS) / Platform

6. **Private System Automatic Location Information (Ali)/Notify**: Based on private system ALi opt-in participation and configuration, SMS notification can be sent to a list of numbers when an E911 or NG 9-1-1 call is made to an agency. This will fulfill the need for some requirements to do "Attendant Notify" of emergency calls, where a PBX or other private system cannot support the function itself.

7. **Support Agency Multicast Audio** - Secure APIs and IoT devices are provided for open third-party vendor support of the ability to use SIPREC recorded audio to be multicast to a participating agency's overhead speakers or dedicated audio sub-system.

   This egress audio integration will be done by SIP and Unicast/Multicast Real-time Transport Protocol (RTP). Using SIPREC at the network level, the recording system and integration NGCS gateway securely support the ability to subsequently subscribe to audio being delivered in near-real time at the same or partnering agency.

   The following describes a use-case example: A fire department wants to hear the calls taken into their dispatch desk in the garage as the responders are preparing to depart. With this new feature, the dispatch desk operators are offered a mechanism to view the calls they are actively taking, or have taken, and can direct the audio to one of multiple zones created by software consoles or hard media devices (for example, SIP phones or overhead speakers). The dispatcher can start, restart, loop, etc. This can include any audio ranging from the instance a call is taken within the participating agency, up to, and even after, it is hung-up, picking the point in time of what to broadcast, to where, and for what period or frequency in a loop thereof. The IoT device support through web service is envisioned for portable devices that would integrate with radio and speaker systems (for example, in vehicles).

SRP 2	**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			
	Bidder Response: Hamilton complies with requirement SRP 2.				

Any additional documentation can be inserted here:

Hamilton adheres to a structured approach to planning and execution of maintenance and configuration updates. Maintenance events include a work and safety plan (WSP) that is created to provide notification and transparency to 9-1-1 system stakeholders. The focus of the WSP is on documenting a primary plan, creating a backup plan, peer review, results verification, and stakeholder identification.

When maintenance work is necessary, Hamilton creates a comprehensive document describing specifically which work needs to be completed and a step-by-step guide on the work that will be completed. Once the maintenance work is complete, a detailed report is provided including the corrective and/or preventative actions taken. These reports will include events by date and time range and specific events.

Defect Resolution software patches and hot-fixes are generally scheduled on an as needed basis. An evaluation will be made by operational and development teams to determine the necessity of a hot-fix or patch. Following those, a defect resolution will be scheduled in an upcoming scheduled release.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SRP 3.				

Any additional documentation can be inserted here:

Hamilton employs rigorous steps to operationally and technically review all new software and patch releases end-to-end. When possible, errors are identified, and the scope and impact of the software defect bug is verified in our Quality Assurance (QA) software testing work group.

The QA group develops and provides a detail of the defect, as well as the specifications needed by the software development teams of how to remedy the defect. Software Development creates a work schedule and deadline, writes the required code and performs initial testing, then hands software back to QA for testing and verification.

Once QA has deemed the software ready for production, the operations team takes over and performs a series of tests and validation that software will behave in the production environment as it did in the QA lab and testing environment. This work is conducted using an in-market test lab.

Once both QA and the ops teams have agreed, the code is ready for production deployment and a Hamilton Work Safety Plan (WSP), or MOP, is distributed to stakeholders for notice and approval. A maintenance window is established, and the upgrade is completed.

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) Commission staff prior to Final Acceptance Testing.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SRP 4.				

Any additional documentation can be inserted here:

Access to Defect Tracking System

Hamilton will provide regular status updates of any relevant defect resolutions as part of the regular cadence of project review meetings. Defect resolutions are tracked either through Hamilton's primary ticket management system, TeamSupport, or through our development team's tracking system. In the event of a defect requiring emergency escalation, Hamilton will provide additional visibility to the state, up to and including pertinent access to Hamilton's system for tracking progress of defect resolution.

Software Defect Tracking Progress

Upon discovery of the software defect and communication by the customer to Hamilton's 24x7x365 network operations center/security operations center (NOC/SOC), a ticket (change request) is created and reviewed by Hamilton NOC/SOC staff. Depending on the severity of the issue, it may be escalated to the development team. The development team will make a determination whether the defect will require a hot-fix, a patch, or a new version release. Once a decision on the resolution is reached, it is slated for release against a specific release or as a priority hot-fix. Training can be provided to Commission staff on the defect tracking process prior to final acceptance testing.

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: Hamilton complies with requirement SRP 5.				

Any additional documentation can be inserted here:

Hamilton adheres to AGILE software development within a Scrum framework. This specific type of software development methodologies is based on iterative development where requirements and solutions evolve through collaboration between cross-functional teams.

Upon discovery of a software defect, a ticket (change request) is created and reviewed by Hamilton NOC/SOC staff. Depending on the severity of the issue, it may be escalated to the development team. The development team will make a determination whether the defect will require a hot-fix, a patch, or a new version release. Once a decision on the resolution is reached, it is slated for release against a specific release or as a priority hot-fix. Training can be provided to Commission staff on the defect tracking process to final acceptance testing.

		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: Hamilton complies with requirement DOC 1.				

Any additional documentation can be inserted here:

Hamilton will provide the Commission with all pertinent documentation for the ESInet and/or NGCS connectivity as part of its implemented solution. All documentation will be provided within 30 days following the completion of the network construction and Hamilton will update the Commission as configurations change over the term of the contract.

Hamilton can provide all documentation in a customer desired soft copy format. Hamilton also utilizes a web-based software portal to provide access to documentation. For example, the state of Nebraska will be provided with access to a web-based portal, NE911.net, that will provide controlled access to 911 Logix, Hamilton's centralized logging system for all critical functional elements and CPE, training and configuration documents, etc. The web client controls both the access to and the inappropriate dissemination of the customer confidential information This documentation will include the following items specified within this RFP question, in addition to other types of documentation:

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-build drawings;
8. PSAP demarcation point drawings; and,
9. All user interface training and reference materials.

Network As-Built Documentation

Hamilton understands that, as the design solidifies and evolves, the "as-built" diagrams will be maintained and supported

to meet Nebraska's requirements. This will include providing a network or solution diagram that clearly depicts Hamilton's solution as implemented. We feel this is a critical component of the service provided in the state and will comply with providing the "as-built" documentation upon implementation.

Hamilton will provide the Commission with all pertinent information for Nebraska's NG 9-1-1 system as implemented and will update the Commission as configurations change over the course of the contract term. As mentioned above, Hamilton can provide all documentation in a customer desired soft copy format. Hamilton also utilizes a web-based software portal to provide access to documentation. For example, Nebraska will be provided with access to a the NE911.net web-based portal providing controlled access to 911 Logix, Hamilton's centralized logging system for all critical functional elements and CPE, training and configuration documents, etc. The web client controls both the access to and the improper dissemination of the customer confidential information. This documentation will include specified documentation listed above, as well as the as-built documentation.

ESI 1	**Emergency Services IP Network (ESInet)** **Diversity** The network shall be designed with diverse entrances (e.g., east-west entrances) into specified buildings that are part of the ESInet. This requirement shall apply to the core network sites, including data centers and PSAPs specified in Attachment A - PSAP Host End-Point Locations, Equipment List and Selective Router Locations. Primary and redundant links shall not share common routes, trenches, or poles. If last-mile facility or building construction is required, bidder shall so indicate. If this is not possible at a given location, indicate how bidder intends to provide redundant and resilient connectivity to that location. Describe how bidder's solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 1.				

Any additional documentation can be inserted here:

The Hamilton solution is designed to ensure 99.999% availability with full redundancy of systems and follows the Communications Security, Reliability and Interoperability Council (CSRIC) best practices and FCC order 13-158.

When possible, Hamilton suggests using a multi-carrier approach for each PSAP. This approach applies to core network sites, including data centers and PSAPs specified in Attachment A – PSAP Host End-Point Locations, Equipment List and Selective Routers. This provides additional diversity beyond physical facilities for the PSAP and beyond what is attainable with a single carrier solution. For example, Hamilton may utilize two connections from two primary providers, where available, and a 4G modem at the PSAP to ensure provider and physical diversity. Each PSAP will be researched and analyzed for the best suitable service providers as the RFP process continues.

Specified buildings will have redundant access systems from two providers where economically practical, and one wired provider and an LTE or FirstNet provider for other locations.

Where route overlap is identified, and diversity is not possible, alternate carriers that can provide service will be evaluated. These alternatives include commercially available internet service providers (DSL, cable, etc.) and wireless (4G/5G) options. The goal is full compliance with the requirement.

Originating service providers (OSPs) will connect at diversely points, at the two data centers or alternately provisioned points of interconnect (POI). Additionally, a tertiary alternate 800# route will be built into the system for call delivery.

Outgoing calls from the ESInet will leverage SIP trunks from diverse carriers at multiple datacenters.

Additionally, an out of band network connection can be established to each PSAP utilizing a Nationwide Public Safety Broadband Network (FirstNet) or comparable services. Exceptions or outliers with limited connectivity options will be documented, along with the development of a risk mitigation strategy.

ESI 2	**Emergency Services IP Network (ESInet)** **Network Design** Bidder shall design the physical network using the most robust facilities available. Use of fiber-optics is the preferred method for connectivity due to available capacity (bandwidth) and increased reliability. Given the amount of fiber-optic facilities and interconnections between the fiber-optic networks in Nebraska, the ESInet design should include as much fiber as possible, not only on the transport side but on the access side as well. Describe the design of proposed network with specific details on connectivity.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 2.				

Any additional documentation can be inserted here:

Hamilton has designed a physical network utilizing the most robust facilities available. Through working with NebraskaLink, Nebraska's statewide fiber optic network providing broadband transport and ethernet access, Hamilton will utilize fiber transport as the main method of connectivity to provide the available capacity (bandwidth) and increased reliability.

As one of the five owners and founding partners, Hamilton is extremely familiar with working with NebraskaLink and has done so for a significant period of time in order to provide unparalleled service to the business community were high reliability and dependability are key. The partnership between Hamilton and NebraskaLink has allowed Hamilton to expand its already broad infrastructure and data transport services. Hamilton plans to work closely with NebraskaLink throughout the course of this project as NebraskaLink can lend their expertise in ordering and provisioning circuits.

Overall, Hamilton's proposed solution utilizes both physical redundancy and geographic diversity in all aspects to ensure a fully redundant solution. For example, each of the two geographically diverse core routing nodes consist of redundant hardware and software for all critical elements. Leveraging both the physical redundancy within each core routing node and the geographically diverse nodes with all hardware operating in an active-active manner ensures that any component failure does not result in an outage of the function it performs. Rather, service uptime remains unaffected as the active resources function without the failed component.

Hamilton also engineers its physical network in the same manner, focusing on physical and geographic redundancy to ensure system uptime remains at 99.999%. This is accomplished by utilizing fiber transport with PBB-TE (Provider Backboned Bridged with Traffic Engineering), and MPLS (Multiple Protocol Label Switching) for diverse network elements. By utilizing two in-state data centers, the Nebraska Data Center (NDC) and Hamilton's data center located at its corporate headquarters, PSAPs will access redundant systems at two geo-diverse data centers as each hosts physical redundant hardware, providing four layers of redundancy. The proposed solution will have diverse fiber paths connecting the two data centers, avoiding single fault domains to the greatest extent possible. Where overlap is identified, alternate and diverse carrier routes, if available, will be added to the network where needed.

Originating service providers (OSP) will connect at two diverse POIs and have an alternate 800 route built into the system for call delivery. Outgoing calls will leverage SIP trunks from diverse carriers. OSPs connecting via SIP can use a SIP option messaging to allow for active calls to be maintained during an outage. The system and services provided by Hamilton supports real-time transport protocol redirects.

The NGCS nodes, functional, and network elements, as well as the services they provide, are self-healing from the call taker perspective. On all known failure states, the redundant and diverse systems will be configured to automatically maintain continuity of service. This is accomplished by having all functional elements in the call chain assigned multiple delivery destinations and A and B geographic redundancy. Additionally, Hamilton utilizes self-healing routing protocols within the ESInet to re-route IP traffic in the event of a circuit failure.

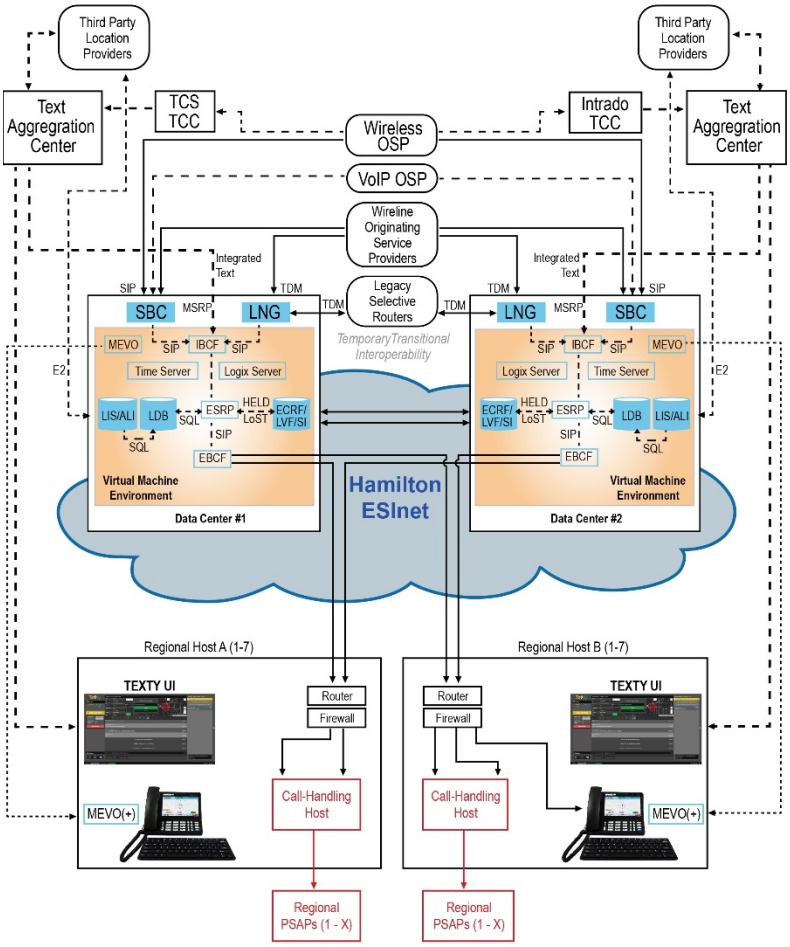
Attaining full redundancy requires the OSP to establish redundant connections to the ESInet. If a carrier is connecting via legacy technology, such as SS7, the carrier would need to support a legacy protocol called crankback, which allows an alternate route to be established if the main connection is impaired. However, some OSPs do not support crankback. Hamilton will make every effort to migrate legacy OSPs to SIP ingress during the transition process.

Additionally, the ESInet to the PSAP is designed to be redundant in all regards. PSAP circuits will be redundant, diverse, employing different network providers where possible. ESInet transport between the core nodes and the PSAP will make use of redundant carrier diverse facilities to the demarcation point at each PSAP. When diverse connections are being deployed, Hamilton will ensure they are always located at diverse entrances in the building to the demarcation point.

However, where diverse carriers with non-diverse entrances to PSAP facilities exist, Hamilton will work to report these instances to the Commission. Each PSAP will have redundant circuit termination routers. The routers will be linked together and provide failover routing techniques such as bidirectional forwarding detection (BFD).

It is important to note that the proposed physical network will not be impacted by events that occur outside of the state because all elements, including the physical network, core routing nodes, data centers, etc. are located within, and dedicated to, the state of Nebraska.

Hamilton has included an image of its proposed solution below, which includes a network design for both transitional and end state. Due to the unique nature of network systems, each network design is specific to client needs and will be engineered to meet those needs. Therefore, the drawing below depicts an initial design for reference. Hamilton understands that, as the design solidifies and evolves, the "as-built" diagrams will be maintained and supported to meet Nebraska's NG 9-1-1 requirements. However, we feel this diagram is a good representation of Hamilton's network design depicting redundant hardware and software for all critical elements.



Hamilton's network design diagram depicting Hamilton's proposed solution.

ESI 3	**Emergency Services IP Network (ESInet)** **No Single Points of Failure** The mission-critical ESInet shall be designed with no single points of failure. All equipment shall include redundant processors and power supplies and be supported by an uninterruptible power supply (UPS) system and alternate power source in a properly conditioned environment. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 3.				

Any additional documentation can be inserted here:

Hamilton ensures there are safeguards to defend against exposure to any single point of failure and to ensure continuity of service.

Hamilton's approach is to design networks to be regional, reliable, and redundant. The engineering of core functional elements keeps those principals in mind. Core functional elements are located in two geographically diverse datacenters. Each functional element is also redundant within each core processing node. All critical hardware elements utilize redundant power supplies to minimize risk of failure due to power interruption.

The network elements providing connectivity between core processing nodes also utilize the same regional, reliable and redundant methodology. Reliability and redundancy are enacted by utilizing diverse carriers, as well as diverse facilities where possible.

The network for delivery of services to the PSAP is also engineered with the same principals and utilizes diverse carrier facilities where possible. Network termination equipment at the PSAP is also redundant to further minimize risk of service interruption.

ESI 4	**Emergency Services IP Network (ESInet)** **IPv4 and IPv6 Support** All network equipment shall be new and of current manufacture at the time of implementation. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IpPv6 and have the capability to run dual protocol stacks. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 4.				

Any additional documentation can be inserted here:

Hamilton's proposed solution includes network equipment that is new and of current manufacture at the time of implementation. Further, all servers, systems, routers, switches, and other network equipment will support IPv4 and IPv6 and will have the ability to run dual protocol stacks.

Hamilton will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards.

All proposed network equipment has the capability to utilize IPv4 and IPv6 and is configurable to support dual stack operation. Some internal systems solely support IPv4, however, this will not be a limitation for the solution proposed by Hamilton. For example, when an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet core will strip down the IPv6 packet, removing the IPv6 header, will add the IPv4 header, and will pass it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. Both the IPv4 network and the IPv6 interfaces are monitored continuously for availability and performance. This is accomplished with the use of a back-to-back user agent (B2BUA) session border controller (SBC), as compared to network address translations (NAT). All devices within the network will be assigned static addresses.

ESI 5	**Emergency Services IP Network (ESInet)** **Open Standards** Open standards-based protocols shall be used, and the use of proprietary routing protocols is prohibited. **Resiliency** Resiliency, or fast failover, may be achieved through the use of the Bidirectional Forwarding Detection (BFD) protocol as defined in IETF Request for Comments (RFC) 5880 and RFC 5881, or other standards-based, non-proprietary methods. Describe how the bidder's solution will achieve resiliency.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 5.				

Any additional documentation can be inserted here:

Open Standards

The proposed system is fully compliant with the open standards requirement. Hamilton is not utilizing any proprietary standards or protocols in the proposed solution.

We adhere to the following, widely accepted, definition of open standards:

- "Open Standards" are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process.
- "Open Standards" facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

The Internet Engineering Task Force (IETF), Institute for Electrical and Electronics Engineers (IEEE), Internet Society (ISOC), World Wide Web Consortium (W3C), and Internet Architecture Board (IAB), jointly affirmed a set of principles which directly contributed to the growth of worldwide technologies based upon the principles of Open Standards. These principles define open standards and establish the building blocks for collaborative innovation.

Standards developed using the OpenStand principles are developed through an open, participatory process, support interoperability, foster global competition, are voluntarily adopted on a global level and serve as building blocks for products and services targeted to meet the needs of markets and consumers.

Public safety, including Next Generation 9-1-1 products and services, need to be built on the principals of open standards and interoperability.

Resiliency

The proposed solution provides resiliency through the use of bi-directional forwarding detection (BFD) at the PSAP edge of the network. For fast failover in the core network, enhanced interior gateway routing protocol (EIGRP) is utilized.

By utilizing border gateway protocol (BGP), bi-directional forwarding detection (BFD), and other open shortest path first (OSPF) routing protocols, we propose to create a self- healing, scalable network. If additional bandwidth or additional survivability is required, it is simple to add additional network connections.

ESI 6	**Emergency Services IP Network (ESInet)** **Multicast Routing and Switching** Routers and switches must support multicast routing and switching. The applicable base protocols are Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 6.				

Any additional documentation can be inserted here:

The routers and switches in the proposed solution support multicast routing and switching, including the protocols Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM).

ESI 7	**Emergency Services IP Network (ESInet)** **Quality of Service (QoS)** The network equipment shall support Quality of Service (QoS) marking for prioritizing traffic in the network using the Differentiated Services Code Point (DSCP) protocol. While the network can change DSCP values through rules, the values typically are set by the system or functional element that originates the traffic. Network routers and switches shall not be configured in such a manner as to change DSCP values set by originating functional elements. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 7.				

Any additional documentation can be inserted here:

Hamilton's proposed solution supports quality of service (QoS) marking for prioritizing traffic in the network using the Differentiated Service Code Point (DSCP) protocol.

Hamilton and its subcontractors currently operate large scale statewide networks in multiple jurisdictions that use these design and implementation approaches. The proposed solution follows the QoS – DSCP markings defined in the NENA i3 standards.

ESI 8	**Emergency Services IP Network (ESInet)** **ESInet Properties** The proposed ESInet shall be private, robust, scalable, secure, diverse, redundant, sustainable, and self-healing. Bidder shall propose a network solution for all host sites listed in Attachment A - PSAP Host End-Point Locations and any future identified regions throughout the term of the contract. Describe how the proposed system meets each of these individual requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 8.				

Any additional documentation can be inserted here:

Hamilton's proposed ESInet will be private, robust, scalable, secure, diverse, redundant, sustainable and self-healing and Hamilton has proposed a network solution that will accommodate all host sites listed in Attachment A – PSAP Host End-Point Locations and any future identified regions throughout the term of the contract. The following explanation provides more specific details regarding Hamilton's proposed ESInet solution:

Private & Secure

Hamilton's proposed ESInet will be private and secure and Hamilton feels these two attributes are closely connected.

Hamilton recommends the deployment of a private core ESInet. Interconnection to "public" networks are established through the use of session border controllers (SBC), virtual public networks (VPN), and other security- related ESInet functional elements.

Hamilton's commitment to security is shown through its compliance with the recommendations and best practices highlighted in NENA document NG-SEC 75-001. In addition, Hamilton has dedicated staff with expertise in network and cyber security. Cyber security is an environment that is ever-changing with new attack vectors, bad actors, and solutions emerging at an increasing frequency. This necessitates concerted systems and procedures to maintain an effective security posture and relationships with commercial and government cyber security-focused organizations.

The proposed solution includes firewalls, border control functions (BCF), and the implementation of access control lists (ACL) at all transitional interface points, including ingress and egress. The firewalls and the transition points they protect will be monitored.

Change controls (CMP) are in place, which require work plans, approvals, testing, coordination, documentation, security risk assessment, etc. Modification made to an ACL or firewall would be considered and governed by this change control process.

In addition to compliance with NENA's NG-SEC standard, the configuration will be in line with industry best practices such as National Institute of Standards and Technology (NIST) standards. Additionally, the proposed security architecture will fully comply with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security policies as Hamilton operates and maintains the NG 9-1-1 network.

The firewalls protect and monitor at layers 2-7. Layer 1, or the physical layer, will be protected by building security measures, such as restricting access and disabling unused ports.

At the data centers, the proposed solution includes service organization control (SOC) 2 Type 2 certified safety and security recommended standards, with 24x7x365 environmental monitoring; video monitoring; dual factor access control; fire suppression system; and individually locked equipment cabinets and cages.

Hamilton has included in the proposed solution a Authentication, Authorization and Accounting (AAA) platform that is integrated into all user interfaces (UI) or portals as presented for use within or outside the ESInet.

The firewall, monitoring, alerting and management information system (MIS) supports a multi-tenant platform with a dashboard function for visibility and control.

Hamilton is fully committed to the NENA i3 standards process and results, but focuses first and foremost on the design and operation of a secure ESInet system.

At the PSAPs, the backroom equipment will include a lockable half rack for the routing and switching equipment. The local area network, call taking positions, and peripherals will rely on the underlying facility access controls and active directory protocols. Hamilton will work to educate and encourage industry best practices to maintain site and network security. Also, Hamilton is highly experienced in completing physical security reports and audits. Hamilton, as part of our nationwide security plan, requires these audits be conducted on our internal network on an annual basis to ensure compliance with applicable statutes, regulations, and policies. Hamilton is willing to enter a contractual relationship to perform in-depth physical security audits, if desired, to ensure overall integrity of security controls and to identify any areas of potential risk and improvement. These audits evaluate physical access, access to critical infrastructure and physical controls, sensitive material handling and many other areas of concern to ensure overall physical security compliance.

In addition, the solution provides a 24x7x365 network operations center/security operations center (NOC/SOC) specializing in 9-1-1 service management. The NOC/SOC utilizes a comprehensive tool set of monitoring applications focused on bandwidth usage, memory usage, CPU usage, and services availability. These platforms for alarms and monitoring vary depending on function and system and include NAGIOS, Statseeker, the Fortinet platform, 911 Logix, and other supporting log subsystems.

Dashboards are utilized to provide comprehensive visibility from all systems listed above. The systems mentioned above and the dashboarding allow for alarms and threshold settings to alert and notify. The notifications can be delivered via visual display, text or email.

Alarming is through both the monitoring platform, the core network and next generation core services (NGCS) event logging sub-systems. The output of these systems is part of our NOC/SOC oversight of the ESInet. Hamilton will work with the Commission to determine the content and frequency of reporting desired for security status and analytics.

The proposed solution utilizes the Fortinet intrusion prevention systems (IPS) within the BCF FE. Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

Telephony denial of service (TDoS) and distributed denial of service (DDoS) attacks can be difficult to identify, especially when originating from legacy OSPs, and require a multi-threaded process to mitigate associated vulnerabilities.

LNGs and SBCs are monitored with threshold detection to identify trunk saturation from the OSP network. Once alarmed, the NOC/SOC will actively identify the source, such as IP address, automatic number identification (ANI), or pseudo automatic number identification (pANI).

If a common source can be identified, it will be blacklisted, and an auto attendant will provide an alternate instruction, or customized delivery to the PSAP for emergency services. If the TDoS/DDoS attack cannot be isolated and live (good) calls cannot be distinguished from the TDoS/DDoS traffic, then other mitigation strategies will be implemented.

These other mitigation strategies vary by the nature of the intrusion and are not fully disclosed in a public facing document (such as this RFP response). They include implementing a honeypot in the call flow to attempt to gather more call location data; requiring a dual-tone multi-frequency (DTMF) response from the caller; using an alternate number; or utilizing an interactive voice response (IVR) system strategy.

As technology continues to advance, the ATIS 'SHAKEN' industry standard is expected to be more commonly available and will be evaluated.
Hamilton has fully developed TDoS/DDoS action plans implemented in other NG deployments. These plans will be a component of the Nebraska implementation plan.

For example, one TDoS Alternate Number Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in a short time span) to listen to an IVR message. This IVR message directs the caller to contact an alternative 10-digit number for their emergency. All other callers are routed to 9-1-1 normally.
The TDoS IVR Mitigation Strategy requires calls/callers flagged as nuisance callers (multiple calls in short time span) to "press 1" to be connected to 9-1-1. All other callers are routed to 9-1-1 normally.

For Multimedia and Text Distributed Denial of Service (MTDDoS) attacks, source IPs flagged as nuisance sources (multiple calls/texts in a short time span) will be filtered using blacklisting and whitelisting. Hamilton will work diligently to blacklist nuisance IP sources. However, if the bad traffic cannot be isolated, then the system will be set to send a bounce back message stating, "Text to 911 is not available at this time, call 911 for service." This will ensure those messages sent by individuals legitimately attempting to reach 9-1-1 by text message do not go unanswered.

At the conclusion of any cyber-attack, and upon resumption of normal operations, documentation of the event will be created. These documents include incident reports, tests completed, lessons learned, and service protections and improvements implemented.

Security is an integral component of Hamilton's roadmap and merits concentrated attention. The following points detail how Hamilton will monitor, detect, analyze, mitigate and respond to cyber threats and adversarial activity on the ESInet:

- Identify ways to further leverage the Information Technology Information Sharing and Analysis Center (IT- ISAC) to help augment cyber security threat detection and mitigation.
- Utilize 911 Logix data analytics artificial intelligence in identification of risks.
- Employ Identity and Credential Access Management (ICAM) standards to create a model for establishing physical security procedures.
- Continued involvement in the advancement of the Task Force on Optimal PSAP Architecture (TFOPA) EC3 concept, as it evolves and becomes a national industry standard.
- Continued integration of technologies supporting Secure Sign On (SSO) and Multi-Factor Authentication (MFA).
- Conduct risk assessment analysis including the typical threat vectors.
- Perform physical security analysis.
- Develop contingency plans.
- Complete an assessment of all liabilities to be used in live testing scenarios. This will ensure the system is protected against real threats.

Robust & Scalable

Hamilton's proposed solution is designed and deployed in a way that is easily scalable and can support significant growth.

The proposed ESInet design will permit scalability as the next generation core services (NGCS) call processing elements are deployed in a virtual machine (VM) environment, providing the ability to add resources as required. Software licensing in this proposal is based on the population of the state of Nebraska. After the project is successfully implemented, the only variance in charges would be related to price-per-population adjustments associated with population increases or decreases.

Hamilton's preferred network design is to utilize the highest quality network providers in each core site, PSAP, or region to develop the most reliable network. Some of the network facilities included in Hamilton's proposed design (e.g. the Hamilton data center) are owned by Hamilton, which allows Hamilton to have ultimate control and supervisory authority over all data center operations. Utilizing the Nebraska Data Center (NDC) and NebraskaLink for circuit transport allows Hamilton to maximize the reliability of our design by using multiple network providers and facilities. In the event that fiber transport circuits are not available, Hamilton's design can utilize IP connections from a cable modem, DSL, 4G LTE/5G wireless, Fiber, and close to any other transport method to create an ESInet.

As mentioned earlier, by utilizing border gateway protocol (BGP), bi-directional forwarding detection (BFD), and other open shortest path first (OSPF) routing protocols, we propose to create a self- healing, scalable network. If additional bandwidth is required, the NebraskaLink primary fiber connections can be upgraded sometimes within minutes. If additional layers of network survivability are required, it is simple to add additional network connections, where available.

The ESInet will use redundant 1Gbps connections between the data centers. The router ports on the core-to-core connections are 1Gbps capable and would not require a hardware change in the event of increased bandwidth requirements. Hamilton has not experienced capacity constraints for transport speeds in excess of 1Gbps for deployments of more than ten times the population and call volumes of Nebraska's current volumes.

Diverse

Hamilton aims to incorporate diversity in several different ways within its ESInet design and believes this is an integral part to designing a network that is regional, reliable, and redundant.

To ensure diverse provider facilities, Hamilton, and its subcontractors, will be working from the following facility locations:

- Hamilton Data Center – 1006 12th Street, Aurora, NE 68818
- Nebraska Data Center (NDC) – 1623 Farnam Street, Omaha, NE 68102

NDC is certified Tier 3 and the Hamilton data center is built to Tier 3 specifications that has been running at better than 99.999% uptime for over 10 years. NDC is operated by a separate entity, ensuring an additional layer of redundancy. These two data centers will serve as redundant cores within the state to maintain 99.999% availability. In addition, these local data centers will serve as the primary points of interconnection (POI) with the originating service providers (OSP) and network providers, as well as the cores for the hosted call-handling facilities. The proposed solution also includes national nodes in two geo-diverse locations. These serve as additional N+1 redundant functional element. This design objective forms a fully redundant system for the in-market nodes.

Each of the two geographically diverse core routing nodes consist of redundant hardware and software for all critical elements and the two geographically diverse data centers will house the core functional elements (FE). Each FE is also redundant within each core processing node. All critical hardware elements utilize redundant power supplies to minimize risk of failure due to power interruption.

The network elements providing connectivity between core processing nodes also utilize the same regional, reliable and redundant methodology. Reliability and redundancy are enacted by utilizing diverse carriers, as well as diverse facilities where possible.

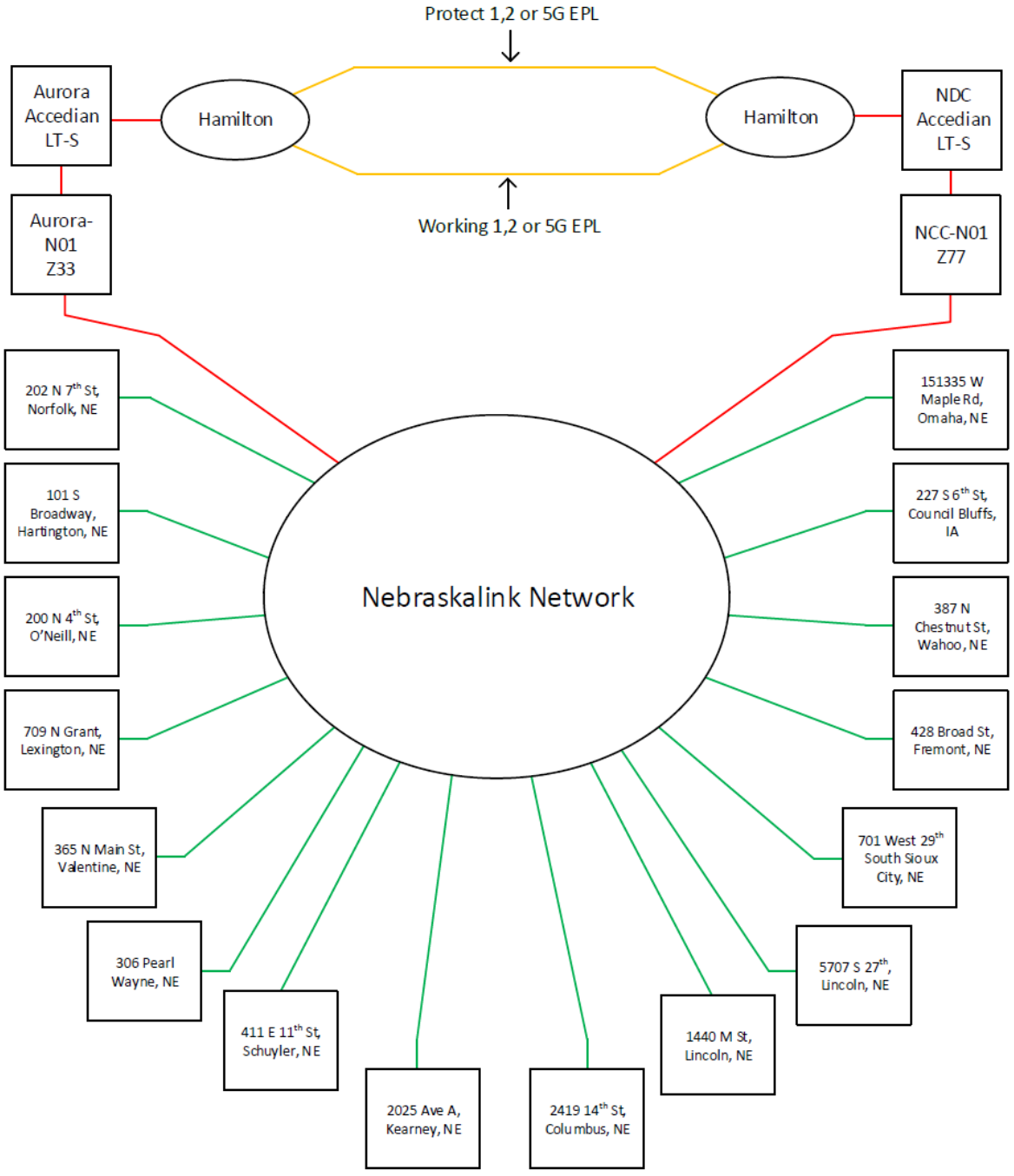
The network for delivery of services to the PSAP will also be engineered with the same principals and utilizes diverse carrier facilities where possible. Network termination equipment at the PSAP is also redundant to further minimize risk of service interruption.

During transition away from the current providers of legacy systems, Hamilton will work with all parties providing 9-1-1 systems service to PSAPs to ensure routing ad delivery of calls to the core CPE and out to the respective PSAP. Overall, the proposed solution utilizes both physical redundancy and geographic diversity to ensure a fully redundant and diverse solution.

Redundant

Hamilton's ESInet design is robust in nature and the proposed solution will provide geo-redundant and locally redundant next generation core services (NGCS). This level of redundancy is achieved through the use of two data centers located in different parts of Nebraska: the Nebraska Data Center (NDC) located in Omaha, NE, and the Hamilton corporate data center located in Aurora, NE.

The proposed solution utilizes both physical redundancy and geographic diversity to ensure a fully redundant solution, making it the most robust available. Each of the two geographically diverse core routing nodes consist of redundant hardware and software for all critical elements, essentially providing four layers of redundancy. In addition, the proposed solution will have diverse fiber paths connecting the two data centers, avoiding single fault domains to the greatest extent possible. Where overlap is identified, alternate and diverse carrier routes will be added to the network where needed. Leveraging both the physical redundancy within each core routing node and the geographically diverse nodes ensures that any component failure does not result in an outage of the function it performs. Rather, service is rerouted around the failed component to other active resources.



Physical and geographic redundancy guarantees that a component failure will allow full capacity at the other node to ensure system uptime remains at 99.999%.

Planned maintenance events are managed in a similar fashion. Utilizing redundant components and geographically diverse nodes, a single node or component can be temporarily decommissioned for maintenance while maintaining full

availability of call routing and call delivery service. This allows component/element maintenance that does not impact the overall service.

The solution offered is highly resilient and reliable, making use of diversity and redundancy for all functional elements used for call delivery, handling, and emergency service functions. Network elements are also diverse and use fiber transport provided by NebraskaLink with PBB-TE (Provider Backboned Bridged with Traffic Engineering) and MPLS (Multiple Protocol Label Switching).

The architecture of the proposed solution will not be impacted by events that occur outside of the region because all elements of the proposed solution will be located within the state of Nebraska. In addition to the core design, Hamilton is providing its disaster recovery system, MEVO(+), as an optional service that allows calls to be delivered out of band from the primary network, as a call delivery point in the event of CPE impairment or failure. MEVO(+) is further detailed within several sections of this response, including Sections 4.1 and 5.21.

The NGCS nodes use the policy routing function (PRF) to automatically reroute calls to the MEVO(+) system in the event of a system impairment or failure. This can also be accomplished at the individual PSAP level, at the regional level, or on a statewide level. Calls can be automatically re-routed to another PSAP, a mobile command center, or the MEVO(+) platform by the PRF function.

Alternatively, PSAPs may request that calls be redirected to MEVO(+) by calling the network operations center/security operations center (NOC/SOC), or by activating the "abandon PSAP switch" by the local authority. This is useful in accommodating scheduled maintenance activities at the PSAP to update all system components. When calls are redirected to MEVO(+) at the PSAP level, MEVO(+) is deployed as a separate VoIP phone at each workstation. The phones are registered over the ESInet to the MEVO(+) server.

Additionally, the MEVO(+) platform can serve as a secure backup call-taking solution providing all pertinent information for a PSAP call taker to effectively handle a 9-1-1 call, plus the added capability of RTT.

Also, the policy routing function (PRF) strategy can include administration lines, cell phones, MEVO(+) phones, and neighboring PSAPs as necessary. Hamilton will make every commercially available effort to deliver 100% of emergency calls, regardless of the circumstances.

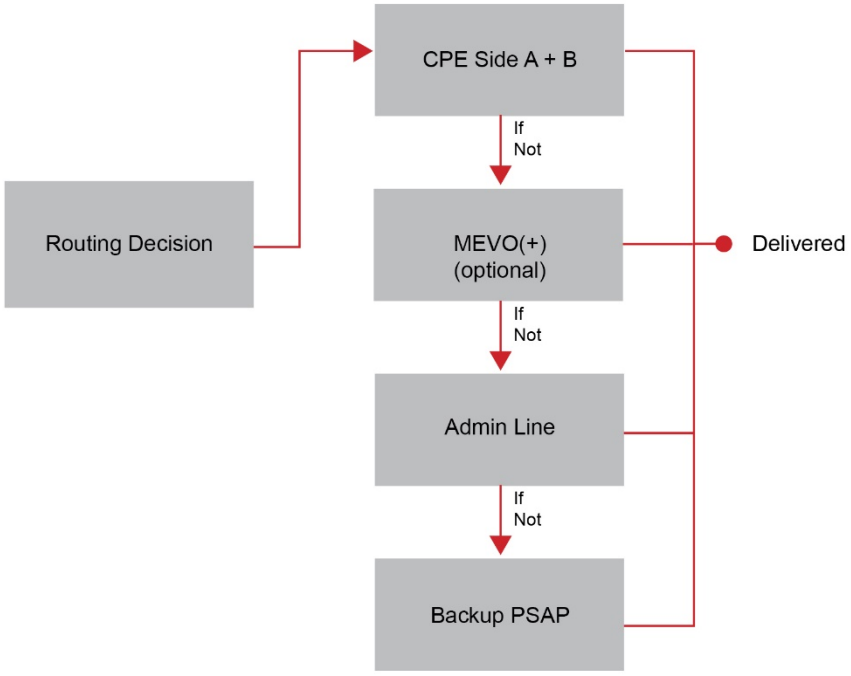
Originating service providers (OSP) will connect at both data centers and have a tertiary alternate 800 route built into the system for call delivery. Outgoing calls will leverage SIP trunks from diverse carriers, if available, at the two data centers. OSPs connecting via SIP can use a SIP option messaging to allows for active calls to be maintained during an outage. The system and services provided by Hamilton supports real-time transport protocol redirects. However, ingress OSP capabilities cannot be determined prior to establishing connections with them.

The NGCS nodes, functional, and network elements, as well as the services they provide, are self-healing from the call taker perspective. On all known failure states, the redundant and diverse systems will be configured to automatically maintain continuity of service. This is accomplished by having all functional elements in the call chain assigned multiple delivery destinations, A and B geographic redundancy, and Hamilton's MEVO(+) continuity service. Additionally, Hamilton utilizes self-healing routing protocols within the ESInet to re-route IP traffic in the event of a circuit failure.

Attaining full redundancy requires the OSP to establish redundant connections to the ESInet. If a carrier is connecting via legacy technology, such as SS7, the carrier would need to support a legacy protocol called crankback, which allows an alternate route to be established if the main connection is impaired. However, some OSPs do not support crankback.

Sustainable

Hamilton includes sustainability within its ESInet design and has included procedures to sustain connectivity in the event of a primary network failure. For example, to ensure that active calls are delivered to the PSAP in the event of a network or mid-call failure, Hamilton utilizes the policy routing function (PRF) to provide alternate routing procedures for call routing in the event of failures in the call flow. The PRF is an integral part of the NGCS system and is the component that enables 99.999% availability. The PRF can be unique to each PSAP, but for the purposes of this response, the most common deployment technique will be illustrated.



The PRF follows a sequential decision tree on where to deliver a call. Typically, calls are delivered to the A side of the CPE interface. In the event the A side is unresponsive, calls are delivered to the B side. If the B side is unresponsive, the emergency services routing proxy (ESRP) continues to use additional PRF business rules until the call is delivered.

There is no limitation on how many destinations can be added to the PRF. The PRF also includes unanswered call timers as well. Once a timer has expired, the call is attempted to the next resource. The PRF/ESRP also behaves differently depending on SIP rejection messages presented by the next device in the call flow, providing a "look ahead" function.

Another critical aspect of call flow is network redundancy and failover. The data centers will be connected via redundant high capacity links from two different providers. Additionally, a third connection will be created via a 4G / 5G connection, utilizing a VPN to maintain security, to sustain connectivity in the event of primary network failure.

Utilizing the PRF to ensure the delivery of calls during a primary network failure is one-way Hamilton has engineered its ESInet solution to ensure sustainability.

Self-Healing

As mentioned earlier within this requirement, the next generation core services (NGCS) nodes, functional and network elements, as well as the services they provide, are self-healing from the call taker perspective. On all known failure states, the redundant and diverse systems will be configured to automatically maintain continuity of service. This is accomplished by having all functional elements in the call chain assigned multiple delivery destinations, A and B geographic redundancy, and by utilizing Hamilton's disaster recovery platform, MEVO(+), which is described above. Additionally, Hamilton utilizes self-healing routing protocols within the ESInet to re-route IP traffic in the event of a circuit failure.

ESI 9	**Emergency Services IP Network (ESInet)** **Special Construction** Bidder is responsible for any fees incurred through system commissioning, construction permits, make-ready costs, and other subcontracted activity. **Use of Existing Network Assets** There is already a microwave network in place that may be used as a backup network, as well as other local and state-owned network assets that may be suitable for inclusion in the ESInet. The final network design may make use of any of these facilities that are determined by the bidder to be suitable for inclusion in the ESInet. The bidder may support the router configuration necessary to make use of these facilities. **Network Design Documentation** Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end-state designs for the ESInet.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement ESI 9.				

Any additional documentation can be inserted here:

Special Construction

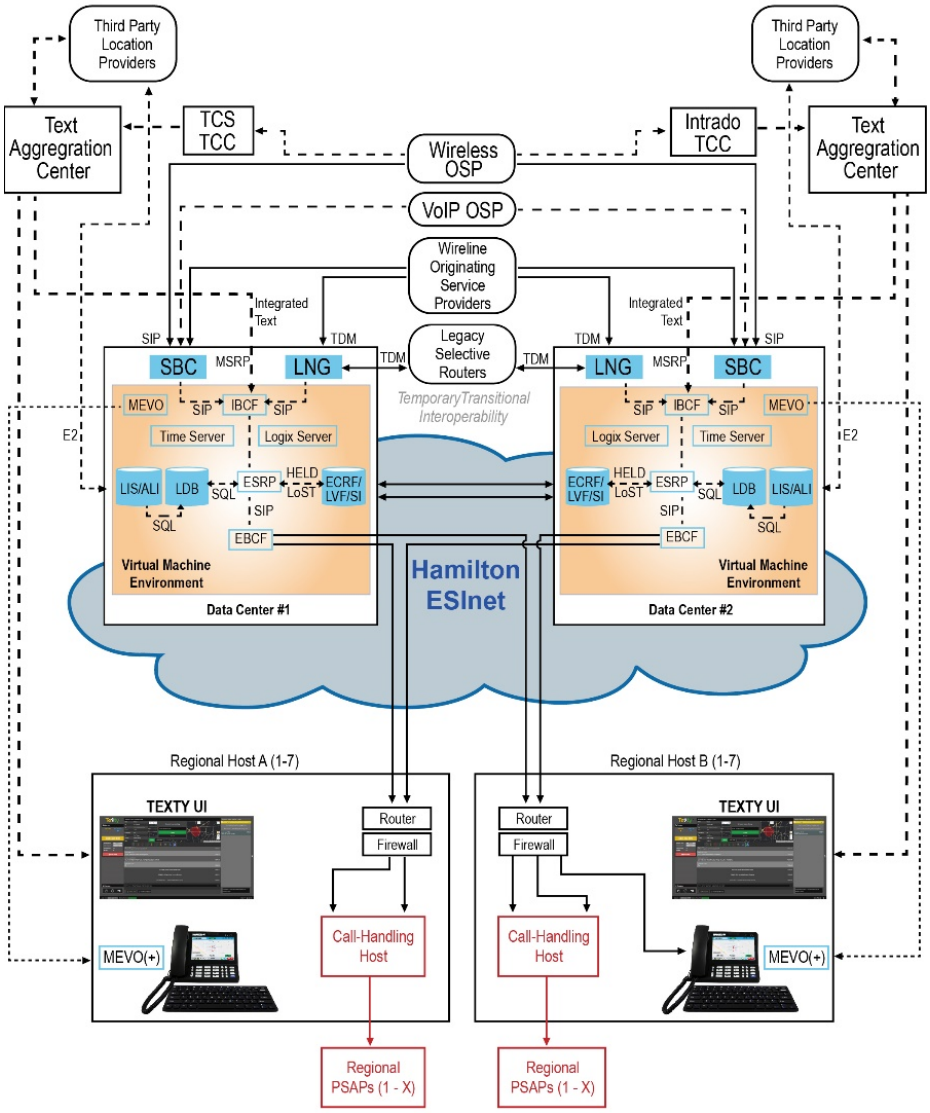
Hamilton will be responsible for any fees incurred through system commissioning, construction permits, make-ready costs, and other subcontracted activity.

Use of Existing Network Assets

As an in-state vendor, Hamilton is very much aware, and informed, on the state's local and state-owned network assets that may be appropriate for inclusion in the ESInet. Hamilton has built its primary and secondary network connections with existing service providers, namely NebraskaLink. As the ESInet project matures, the state's microwave network will be further analyzed for use as a backup network.

Network Design Documentation

The drawing below depicts an initial design for reference. However, we do feel that this network diagram clearly depicts Hamilton's transitional and end-state design for the ESInet. Hamilton understands that, as the design solidifies and evolves, the "as-built" diagrams will be maintained and supported to meet Nebraska's requirements. We feel this is a critical component of the service provided in the region.



ESI 10	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** Contractor shall provide an ESInet solution capable of interfacing with neighboring state and regional NG911 IP networks as they are established, and capable of transferring voice and data between PSAPs. Describe how the solution will meet these requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement ESI 10.				

Any additional documentation can be inserted here:

Hamilton's proposed ESInet solution is capable of interfacing with neighboring state and regional NG 9-1-1 IP networks as they are established, and is capable of transferring voice and data between PSAPs.

To support these transfers to neighboring state and regional NG 9-1-1 networks, Hamilton has identified the selective router locations within the neighboring states for interconnection and delivery of transferred wireless calls. Bi-directional trunking with PSAP to PSAP transfer capability will be established with these out-of-state selective routers to facilitate network-to-network transfers. This will be accomplished via documented standards and best practices.

Hamilton has experience in these matters and has developed the required commercial agreements and industry relations to reach this goal in multiple jurisdictions. In addition, Hamilton will provide the necessary interagency training and coordination of these types of connection arrangements.

In addition to trunking, wireless pseudo automatic number identification (pANI) ranges will need to be shared between each 9-1-1 service provider to facilitate the transfer of additional call data between the PSAPs. Some normalization of pANI ranges between the originating service providers (OSPs), their third-party providers, and the 9-1-1 service providers may be required if there are overlapping ranges. Hamilton believes that establishing connections to these selective routers from the Nebraska 9-1-1 network is the most cost-effective solution.

If selected as the state network operator, Hamilton would establish both IP network-to-network interface agreements (NNI) and legacy E9-1-1 connection arrangements to all border states, both initially during the term of the service contract and as other states modernize their 9-1-1 service. This would be accomplished through the use of both IP and legacy TDM SS7 circuits to integrate border state 9-1-1 systems with the Nebraska ESInet. Additionally, Hamilton will coordinate automatic location identification (ALi) integration with neighboring providers to enable call transfers from the Regional Call Host (RCH) PSAPs with associated caller location data.

Overall, network-to-network interconnections will be established between existing ESI networks. These interconnections will be established using the guidelines set forth by applicable NENA standards. Hamilton and its subcontractors have extensive experience in the successful interconnection of ESInets.

The solution proposed by Hamilton, including all NNI devices, complies with all applicable industry standards.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 11	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** **Connecting to Other IP Networks** At such time as neighboring ESInets and NGCS systems are able to interconnect and exchange traffic, Contractor shall establish such connections and provide routing and security to allow traffic to be exchanged with neighboring ESInets and NGCS systems, regardless of the respective vendors of those systems. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: Hamilton complies with requirement ESI 11.				

Any additional documentation can be inserted here:

As required, Hamilton will work with other ESInet vendors with neighboring state and regional NG 9-1-1 deployments as they are established to transfer voice and data between the PSAPs. Hamilton has an extensive portfolio of experience in these matters and has developed the required commercial agreements and industry relations to reach this goal. In addition, Hamilton's ESInet is designed to be interconnected via industry standard interfaces to any number of adjacent or nearby ESInets.

In addition to trunking, wireless pseudo automatic number identification (pANI) ranges will need to be shared between each 9-1-1 service provider to facilitate the transfer of additional call data between the PSAPs. Some normalization of pANI ranges between the originating service providers (OSP), their third-party providers, and the 9-1-1 service providers may be required if there are overlapping ranges.

When interconnecting with other ESInets, Hamilton will work with the vendors/providers of the ESInets to decide how to best collaborate to determine the appropriate interconnection points with the Hamilton ESInet. Thorough non-live interoperability testing will be completed prior to supporting live emergency calls.

Hamilton has included the costs and has the required intercompany agreements needed for the interconnection and operation of neighboring IP and TDM E9-1-1 networks to support interoperability.

In addition, Hamilton has significant experience interfacing with other i3-compliant ESInets as a statewide NG 9-1-1 service provider. If selected as Nebraska's NG 9-1-1 service provider, Hamilton would establish network-to-network interconnections with existing ESInets utilizing guidelines as set forth by applicable NENA standards. In accomplishing this goal, Hamilton establishes both IP network-to-network interface agreements (NNI) and legacy E9-1-1 connection arrangements to all border states, both initially during the term of the service contract and as other states modernize their 9-1-1 service. This would be accomplished through the use of both IP and legacy TDM SS7 circuits to integrate border state 9-1-1 systems with the Nebraska ESInet. Additionally, Hamilton will coordinate automatic location identification (ALi)

integration with neighboring providers to enable call transfers from the Regional Call Host (RCH) PSAPs with associated caller location data.

Overall, network-to-network interconnections will be established between existing ESInets and Hamilton is fully capable of accomplishing this goal in a seamless manner. Again, these interconnections will be established utilizing the guidelines set forth by applicable NENA standards and the Hamilton team has extensive experience in the successful interconnection of ESInets.

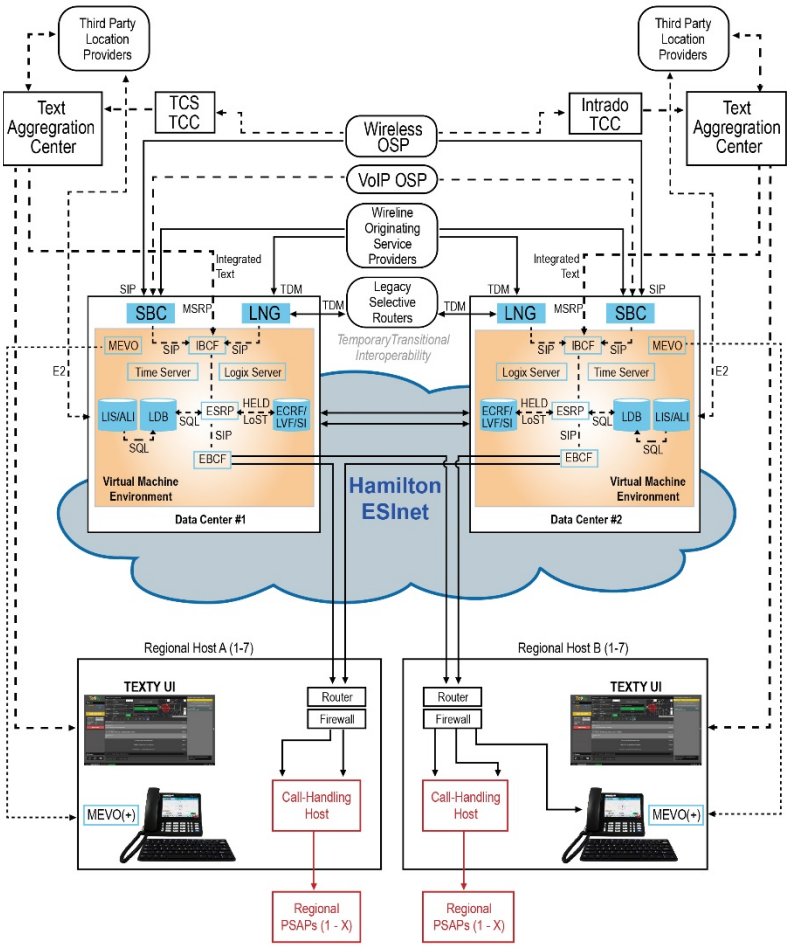
Hamilton has experience in these matters and has developed the required commercial agreements and industry relations to reach this goal in multiple jurisdictions. In addition, Hamilton will provide the necessary interagency training and coordination of these types of connection arrangements.

		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 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: Hamilton complies with requirement NGCS 1.				

Any additional documentation can be inserted here

Next Generation Core Services Elements (NGCS)

The drawing below depicts an initial design for reference of both Hamilton's proposed transitional and end state for the Commissions ESInet and NGCS. This diagram takes into account the hosts and PSAPs included in Attachment A – PSAP Host End-Point Locations, as well as the functional elements and services listed above.



Hamilton's network design diagram depicting Hamilton's proposed solution.

Due Authorization

Hamilton NG911, Inc. has a Certificate of Public Necessity issued on June 2, 2020. Hamilton has provided a copy of its current certificate of public necessity and it is attached as Appendix 16 – Hamilton Certificate of Public Necessity.

Identification of Service Providers Connected to the Legacy Selective Router

Hamilton will work closely with all service providers to facilitate a smooth transition from the legacy network to the next generation ESInet. This will include being responsible for identifying, and connecting, all wireline, wireless, Voice over IP (VoIP), telematics, and other third-party service providers currently connected to the existing legacy selective router. In addition, Hamilton will take responsibility for updating this information quarterly for the term of the contract.

Hamilton, in cooperation with INdigital, has years of experience and working collaboratively with service providers and we currently have interface agreements with local exchange carriers in the Midwest, South East and East. We look forward to working with the carriers in Nebraska.

Regarding third-party location providers specifically, Hamilton already has connectivity established with third-party location providers in the industry. As provider of automatic location identification (ALI) services, we currently have direct relationships with providers. Our ALI systems are connected to West, Comtech and Bandwidth, as well as supplemental provider Rapid SOS. These connections allow for updated location information and rebids during call processing.

Upon contract award, Hamilton will plan and hold kickoff meetings, including all stakeholders, and will create conversion plans. These meetings will encourage collaboration of all stakeholders to facilitate conversion plans and will aid in a smooth and successful transition.

The conversion plan will outline the design, installation, testing, interconnection, and operation of ESInet components required to operate or support the operation and will include network drawings; information on circuit ordering; the different points of interconnections, and project team contact information.

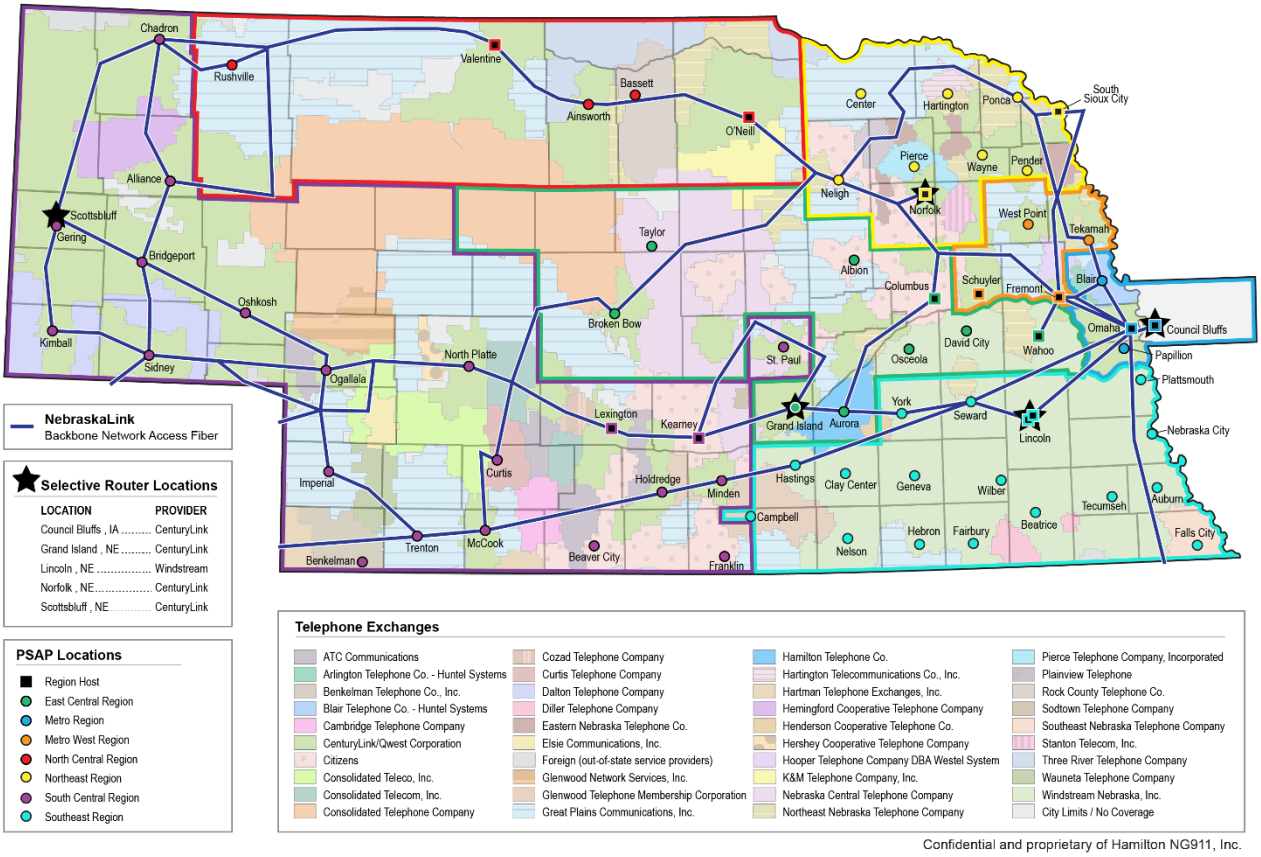
Operation of the ESInet, incorporated in the offered service, will include maintenance and repair of all elements. Furthermore, Hamilton has worked with the majority of national originating service providers (OSP) in other next generation (NG) projects or market areas. Included with this response is a template of a project plan outlining the design, installation, testing, interconnection and operation of the ESInet components. This can be found in Appendix 11 –Nebraska Project Plan Template.

Coordination with the Commission or the Commission's designee will include a weekly project call to review the project status and next steps. Additionally, comprehensive project plans will be provided to all pertinent parties. The project plans will be updated on a daily basis or as critical project tasks are completed. A web share will be established in order to provide pertinent parties with the ability to review all project plans in real time.

In order to best coordinate with all OSPs, Hamilton will schedule project kickoff calls to discuss the project plan and answer any questions. In addition, periodic status calls with OSPs would be established to maintain steady progress and limit potential delays in conversion.

Hamilton is accustomed to working closely with other service providers as necessary to ensure a smooth transition and delivery of networks and systems. Hamilton will operate and provide a seamless NG 9-1-1 service for all PSAPs in Nebraska during the transitionary period.

Nebraska PSAP/ILEC Map



Another division within Hamilton, Hamilton Telephone Company, began as a local telephone cooperative serving Hamilton County, Nebraska, in 1901. Hamilton has deep roots as both a telephone and 9-1-1 services provider, working frequently with other local exchange carriers (LECs), rural local exchange carriers (RLECs), competitive local exchange carriers (ILECs), all wireless carriers, VoIP carriers and other 9-1-1 call sources. Hamilton is fully confident that we can work effectively with all OSPs in Nebraska in order to accomplish a successful transition to the NG 9-1-1 system.

In addition, NebraskaLink is one of Hamilton's main sub-contractors for the completion of the Nebraska NG 9-1-1 project. Hamilton is one of five owners of NebraskaLink, a statewide fiber optic network providing broadband transport and ethernet access across the state of Nebraska and beyond. This infrastructure and investment allow for unparallel service to the business community where high reliability and dependability are key. NebraskaLink offers diverse, robust, and innovative solutions at

competitive rates with an emphasis on provider-class internet connectivity and multi-site architecture. NebraskaLink is owned and operated in Nebraska, with Hamilton being one of five owners. The partnership between Hamilton and NebraskaLink has allowed Hamilton to expand its already broad infrastructure and data transport services. Overall, Hamilton's experience thus far in working with NebraskaLink and the service providers in Nebraska make Hamilton uniquely qualified for this project. Hamilton already has the relationships developed to work with the state's service providers and is familiar with what is required to serve rural areas. Hamilton is passionate about the services and value we can bring to our customers and the constituents of Nebraska.

As the chosen vendor, Hamilton would provide a letter of authorization (LOA) to the Commission to provide Hamilton with the authority to request 9-1-1 trunking orders. Additionally, in order to successfully make this transition and cooperate with existing OSPs, Hamilton will provide OSPs with a project plan that includes drawings, documentation, and a schedule to provide all necessary information needed to establish redundant points of interconnection with the 9-1-1 system service provider.

When interconnecting with OSPs, Hamilton will abide by all applicable federal and Nebraska state laws and administrative rules. Hamilton will file bona fide requests for connectivity with all phone providers, such as all LECs, CLECs, RLECs, ILECs, wireless carriers, VoIP carriers, and any other 9-1-1 call source as identified by the Commission for interconnection to and processing by the NG 9-1-1 system as required by law. Hamilton will cover the expense for any costs associated with these interconnections.

		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: Hamilton complies with requirement NGCS 2.				

Any additional documentation can be inserted here

Hamilton will comply with negotiating interconnection or commercial agreements, and with completing data and network connection agreements with each service provider identified in requirement NGCS 1. These interconnection or commercial agreements will cover subjects such as split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and NGCS, Local Number Portability (LNP), National Number Portability (NNP), Function of Code R (FoCR), and more.

If selected as the state's NG 9-1-1 provider, Hamilton would establish both IP network-to-network interface agreements (NNI) and legacy E9-1-1 connection arrangements to all neighboring jurisdictions necessitated to maintain the required transfer and interoperability operations. This would be accomplished through the use of both IP and legacy TDM SS7 circuits to integrate neighboring systems with the Nebraska ESInet. Additionally, Hamilton will coordinate automatic location identification (ALI) integration with neighboring providers to enable PSAP to PSAP call transfers with associated caller location data. These interconnections will be established using the guidelines set forth by applicable NENA standards.

Hamilton will fully cooperate with all entities involved in providing 9-1-1 services in Nebraska. This will include PSAPs, the originating service provider (OSP), the Commission, network providers, etc. ("stakeholders"). In creating network-to-network interface (NNI) agreements, responsibilities for network security, management, and monitoring functions between the designated network authorities will be defined.

Hamilton has years of experience and history meeting these requirements. We currently have interface agreements with local exchange carriers in the multiple jurisdictions across the country.

The proposed solution includes connectivity with the third-party location providers in the industry including West, Comtech and Bandwidth, as well as supplemental provider Rapid SOS. These connections allow for updated location information and rebids during call processing.

As the chosen vendor, Hamilton can provide a sample letter of authorization (LOA) to the Commission that would provide Hamilton with the authority to request 9-1-1 trunking orders. Additionally, in order to successfully make this transition and cooperate with existing OSPs, Hamilton will provide OSPs with a project plan that includes drawings, documentation, and a schedule to provide all necessary information needed to establish redundant points of interconnection with the 9-1-1 service provider.

When interconnecting with OSPs, Hamilton will abide by all applicable federal and Nebraska state laws and administrative rules. Hamilton will file requests for connectivity with all phone providers, such as all LECs, CLECs, RLECs, ILECs, wireless carriers, VoIP carriers, and any other 9-1-1 call source as identified by the Commission for interconnection to and processing by the NG 9-1-1 system as required by law. Hamilton will cover the expense for any costs associated with these interconnections.

As mentioned above, Hamilton has extensive experience negotiating interconnection agreements. From our experience, we have learned that the negotiating process is dependent upon cooperation from all parties. In order to encourage cooperation between all involved and meet designated timelines, Hamilton approaches interconnection as early in the process as possible, often sending requests for interconnection prior to the official award of a contract. In many instances this has been successful. However, in others, incumbent providers have chosen not to participate in a negotiation until a contract has been finalized.

Typically, we establish a kickoff meeting and provide initial documentation including Points of Interconnect (POIs) and other relevant network information. The kickoff meeting is followed by a series of regular meetings to review interconnection documents, methods and procedures.

Negotiated interconnection is a required step in implementation and Hamilton's goal is to always complete this step in a timely manner. Hamilton has found that the difficulty lies in accelerating the process. The most successful mitigation strategy has been to seek to find compromise solutions that work to move the project's goals and objectives forward while still meeting goals and objectives for the other provider. The ability and willingness to compromise has been a distinguishing characteristic of our past success.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 3.				

Any additional documentation can be inserted here

Hamilton shall be responsible for all facets of the OSP migration project, include managing all moves, adds, changes and deletion of connections from the OSPs to the state's NGCS. The OSP ingress function of Hamilton's NGCS solution can accommodate both TDM and IP technologies. OSPs that can deliver native IP based traffic are inherently easier to migrate to the ESInet and NGCS. Hamilton has the unique ability, via NebraskaLink, to aggregate nearly every legacy OSP that may only be able to deliver their emergency calls in legacy TDM format. With NebraskaLink possessing physical connections to nearly every OSP in the state, Hamilton will obtain all traffic from the OSPs at the edge of their network in whichever format they desire to deliver it in. The TDM traffic will be converted to IP before traversing the Hamilton ESInet and ingressing to the NGCS core. While the typical conversion timeline for each OSP is approximately six (6) months from notification to cutover, Hamilton expects a much faster conversion due to NebraskaLink's existing network. Following each connection made to the network, monitoring is established and must be in place prior to testing and live traffic.

After the initial OSP conversion process has been completed, Hamilton will be responsible for dynamically managing the ESInet as OSPs change technologies, migrate to different POIs, or enter/exit the market. This will be managed through a similar process and effective project management practices.

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: Hamilton complies with requirement NGCS 3.				

Any additional documentation can be inserted here

As a large ESInet provider, Hamilton has learned the importance of minimizing fault domains. This starts during the design and implementation process. Minimizing fault domains begins with the engineering principle of utilizing a distributed network architecture. Our approach moves the functional elements (FE) and network elements (NE) to the edge of the network, limiting the potential for a point of failure to a PSAP or smaller region instead of affecting large geographical areas.

The same design carries over into our approach with legacy network gateway (LNG) FEs. By utilizing the LNG systems that are distributed and non-centralized, we can minimize the effects of ingress trunking failures. This in-state distributed architecture allows the originating service providers (OSP) to connect to the ESInet at the point of interconnect (POI) that works best for them and opens the possibility of the OSP to use multiple networks to connect to the LNG sites.

The LNG collects full detail on all calls received on time-division multiplexing (TDM) interfaces and transmitted to upstream IP interfaces. LNG call detail is transmitted real-time to the ESInet management system for reporting and analysis. This system allows for ad hoc uploads of log files for troubleshooting and incident response.

The proposed solution is built to withstand attacks, including distributed denial of service (DDoS), and Hamilton's security architecture utilizes defenses to protect against these types of sophisticated attacks. Multiple defenses are used to safeguard against the effects of these attacks, including intrusion detection systems (IDS) with DDoS support to protect specifically against these types of attacks. The Hamilton ESInet design limits exposure by keeping the ESInet private and segmenting firewalled touchpoints to the Internet or external domains.

The Hamilton solution is built to withstand sophisticated attacks, including distributed denial of service (DDoS). Hamilton's security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, network intrusion detection and prevention (IDS/IPS), multi-factor authentication, strong encryption, antivirus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only necessary protocols/destinations, for both ingress and egress. The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or access control lists (ACL). Hamilton continually investigates and upgrades new advances in protective technology with tools such as intrusion detection systems (IDS).

The solution incorporates physical, network, and application security principals. Traffic between core processing sites and distributed sites, such as LNGs, is route and protocol secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution.

The proposed LNGs are telco grade central office equipment supporting up to 1,024 SS7 trunks per gateway. The LNGs are manufactured by Sangoma (formerly Dialogic) and Audiocodes, and they meet the requirements for all modern SIP applications.

The LNGs will provide a bridge between the existing legacy 9-1-1 call origination network and ESInet. This is accomplished by primarily using integrated services digital network user part signaling system seven (ISUP SS7); and where required, using centralized automatic message accounting (CAMA) connections to the selective router or directly to legacy OSPs. The LNG will be required in the ESInet if OSPs use legacy technology in their networks.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 5.				

Any additional documentation can be inserted here

Legacy Network Gateways (LNG) with Legacy Selective Router Gateway (LSRG) Functionality

Deployment of legacy selective router gateways (LSRG) is a critical step to a successful transition. Hamilton is proposing to install LNGs with LSRG functionality in a redundant manner to provide a connection to each legacy selective router. These connections will facilitate the transfer of voice calls with ANI/ALI from the legacy network to the ESInet or vice versa. These elements are required throughout the duration of the transitional phase and could be removed when all ingress traffic is transitioned from the legacy networks to the ESInet.

Transition Timelines & Network Costs

Hamilton will take the necessary steps to meet transition timelines and minimize overlapping network costs. In order to achieve this goal, Hamilton utilizes an overlapping, staged approach. NG 9-1-1, by its design, inherently supports the modular transition of service. The ability to provide both full E9-1-1 legacy and NG 9-1-1, as it exists today in a transitional network, at the same time is critical to the success of the project. This parallel approach supports full interoperability between the new and legacy 9-1-1 networks.

Hamilton, via the NebraskaLink network, has existing network connections to nearly every legacy and cellular OSP in the state. With these NNIs already established, a significant first step in the process is already in place. The ability to route emergency calls away from the Legacy Selective Routers, to the ESInet, is a matter of effective project management. After the NGCS cores are established, the timelines for ESInet network provisioning and OSP cutover is much easier than in some state projects that have been stricken with long conversion timelines and dual payment obligations.

Many OSPs do not have the flexibility or resources to support service delivery to both the legacy E9-1-1 system and the new NG 9-1-1 system. Because of these limitations, Hamilton takes a very structured, time-proven approach in our work and has successfully transitioned hundreds of OSPs from legacy systems to NG platforms.

In order to be successful, we begin by establishing new connections to the legacy E9-1-1 selective routers, along with a star code or pANI routing alias. In addition, we hold a kickoff meeting for originating service providers (OSP) to resolve open issues that would prevent an OSP from ordering new connections. We use LNG systems that are distributed and non-centralized. This minimizes the effects of ingress trunking failures.

This in-state, distributed architecture, combined with national service platforms providing service continuity, allows the OSPs to connect to the ESInet at the point of interconnection (POI) that works best for them. This opens the possibility for the OSP to use the best type of connection arrangements to provide diversity and improved service quality.

This approach applies whether the connection is using SS7 trunking or SIP connection arrangements. Our approach utilizes the best available hardware in the market and is based on time-proven platforms that lead the industry in MTBF/MTTR metrics. Full support for all current and emerging protocols used by the OSPs provides the broadest support for public safety services of all types. OSPs can choose to connect to the NGCS nodes using almost any protocol, further ensuring service continuity.

Hamilton, as a current 9-1-1 service provider, will evolve the ESInet from the beginning through the end state with the refinement and progression needed to advance 9-1-1 service for Nebraska. Hamilton will provide both legacy TDM and NG 9-1-1 compliant services during the term of the agreement.

Hamilton establishes new connection arrangements with the legacy 9-1-1 statewide service providers. These are bi-directional facilities, and we can fully manage and emulate all types of legacy signaling protocols for both voice payload and ALI data flows. Hamilton has a complete understanding of legacy SS7 interoperability and NG IP interoperability methods, allowing us to provide a seamless transition for the OSP, the 9-1-1 SSP and the Regional Call Hosts. This RFP requires support for all types of 9-1-1 services. From inception to the final evolution of the ESInet, Hamilton has the proven skills to support the Host Site PSAPs in the transition from a legacy E9-1-1 to a NG 9-1-1 state. During the contract term, the ESInet will continue to evolve and Hamilton will work collaboratively with the Commission to deploy and accommodate emerging technologies.

NGCS 6	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 6.				

Any additional documentation can be inserted here

Experience Working with Legacy OSPs

Hamilton has experience working with legacy originating service providers (OSP) on similar projects and Hamilton will work closely with all OSPs to facilitate a smooth transition from the legacy network to the next generation ESInet.

The process will begin by provisioning trunks from the existing legacy selective routers to the legacy selective router gateways (LSRG) linked to the next generation core service (NGCS) nodes. This ensures that calls can be transferred between the ESInet and the legacy network during the transition period.

Concurrently, Hamilton will identify all current OSPs and begin notifying the OSPs of the pending transition. A series of project introduction calls will be hosted before beginning to work individually with each OSP to transition their traffic from the legacy network to the ESInet.

OSPs will be encouraged to connect to the ESInet via session initiation protocol (SIP). However, when SIP interconnection is not available, legacy network gateways (LNG) will be deployed to accommodate legacy interconnection types. Points of interconnection (POI) will be provided to the OSPs at the core NGCS nodes within the state of Nebraska.

Hamilton acknowledges that significant coordination and collaboration will be needed to successfully make the transition to NG 9-1-1 for the state of Nebraska and working closely with existing OSPs in a manner that facilitates communication, collaboration, and teamwork toward shared goals and objective will ensure this transition is successful.

In addition, Hamilton acknowledges its responsibility as the NG 9-1-1 service provider to create the legal agreements, configuration, and interfaces between the OSPs and other carriers and accomplish this transition in a timely manner. This expertise in carrier transition and subsequent coordination will be integrated into Hamilton's overall approach, which will maximize efficiency and minimize risk during the transition period.

Comprehensive project plans will also be provided to all pertinent parties. The project plans will be updated daily, or as critical project tasks are completed. A web share will be established in order to provide pertinent parties with the ability to review all project plans in real time.

In order to best coordinate with all originating service providers (OSPs), Hamilton will schedule project kickoff calls to discuss the project plan and answer any questions. In addition, periodic status calls with OSPs would be established to maintain steady progress and limit potential delays in conversion.

Hamilton has developed a successful migration schedule to ensure mitigation of any risk and to be able to adapt to any unforeseen schedule delays. As discussed throughout many sections of this proposal, the Hamilton team believes strongly in approaching the transition in planned phases, consistent with the stages defined by the Commission and coupled with our team's extensive experience in migrating customers from legacy infrastructures to advanced, next generation environments.

Hamilton's expert staff focus on the transitioning of NENA i3 NG 9-1-1 services into production with a strong "do no harm" philosophy to ensure ongoing legacy and new NENA i3 operations are not adversely affected during the migration process. This philosophy, first-and- foremost, prioritizes a safeguard approach to current operations. Through our

experience in transitions of comparable size and scope, Hamilton brings the requisite discipline, control, risk mitigation, and organizational subject matter experts necessary to ensure a successful transition for the state of Nebraska.

Configurations to support the migration from both the current transitional and NG 9-1-1 systems to the Hamilton NG911 system will go through rigorous testing and acceptance.

Hamilton will apply proven program and change management best practices that are compliant with both the PMBOK and Hamilton operational standards; ensuring tested and accepted configurations are documented and incorporated into a configuration baseline to ensure successful transition into the production environment. The following system-builds and testing will occur separate from ongoing operations:

- Staging and testing, including simulated PSAP positions.
- Move, install, and test data center systems.
- Build and connect ESInet wide area network (WAN) core and backhaul connectivity between data center sites.
- Build connections to all carriers, allowing ingress emergency services traffic to both data centers. Test circuits onto ESInet.
- Build individual PSAP ESInet WAN connectivity (e.g. access loop) to support migration schedule.
- Build PSAP internal networking environment, testing connectivity to data centers. PSAP IP network equipment instantiation.
- Perform cutover of CAMA trunks for those PSAPs not currently on the deployed Nebraska NG 9-1-1 system, by migrating carrier routing from terminating at PSAP to terminating at data center.
- Test live operation; perform roll-back if required.

This parallel system configurations and testing approach will ensure all environments are ready for transition into production, while simultaneously ensuring no interruption to ongoing operations will occur.

In addition, details of the proposed migration plan are contained in Appendix 11 - Nebraska Project Plan Template. The plan carefully considers the need to maintain 9-1-1 services throughout the migration process. Significant steps are taken to notify existing originating service providers (OSP) of the migration. Hamilton will work closely with the OSPs to coordinate the provisioning of new facilities to the next generation core services (NGCS) and coordinate the decommissioning of legacy 9-1-1 system elements.

The Nebraska Project Plan Template also outlines the careful consideration to the need to coordinate the migration with other system vendors at each Regional Call Host (RCH). Steps are taken to coordinate and inform other vendors, such as call handling, computer aided dispatch (CAD), radio, recording, etc. of the migration. Transparency and continuity of service at the RCH is a primary objective of the plan.

Working with Service Providers in Nebraska

As an established in-state provider, Hamilton is already familiar with the state's existing legacy 9-1-1 service providers and has a long history of working collaboratively with these existing providers. Hamilton is an active member of the Nebraska Telecommunication Association (NTA) and regularly participates in meetings and events with the goal of enhancing its professional relationship with other providers, as well as strengthening telecommunications services for the citizens of Nebraska. Hamilton believes it has a significant number of local assets and resources available and will capitalize on these available assets to ensure that our work with the state's legacy 9-1-1 service providers is a success. In addition, Hamilton's sister company, Hamilton Relay, has ensured that 9-1-1 calls get routed correctly to multiple states, countless PSAPs, and within numerous types of environments and has successfully been routing these emergency calls for decades. The state will find that there is no other bidder more qualified than Hamilton to work collaboratively, and successfully, with Nebraska's established legacy 9-1-1 service providers.

Hamilton will work closely with all originating service providers (OSP) to facilitate a smooth transition from the legacy network to the next generation ESInet. Unique to Hamilton is its considerable amount of experience working with established legacy 9-1-1 service providers within the state. Another division within Hamilton, Hamilton Telephone Company, began as a local telephone cooperative serving Hamilton County, Nebraska, in 1901. Hamilton has deep roots as both a telephone and 9-1-1 services provider, working frequently with other local exchange carriers (LECs), rural local exchange carriers (RLECs), competitive local exchange carriers (ILECs), all wireless carriers, VoIP carriers and other 9-1-1 call sources. Hamilton is fully confident that we can work effectively with all OSPs in Nebraska in order to accomplish a successful transition to the NG 9-1-1 system.

In order to accomplish this goal, Hamilton has established the following roadmap approach for the transition of OSPs from the current legacy 9-1-1 system to the NG 9-1-1 solution proposed by Hamilton within this RFP:

The process will begin by provisioning trunks from the existing legacy selective routers to the legacy selective router gateways (LSRG) linked to the next generation core service (NGCS) nodes. This ensures that calls can be transferred between the ESInet and the legacy network during the transition period.

Concurrently, Hamilton will work with all current OSPs and begin notifying the OSPs of the pending transition. A series of project introduction calls will be hosted before beginning to work individually with each OSP to transition their traffic from the legacy network to the ESInet.

OSPs will be encouraged to connect to the ESInet via session initiation protocol (SIP). However, when SIP interconnection is not available, legacy network gateways (LNG) will be deployed to accommodate legacy interconnection types. Points of interconnection (POI) will be provided to the OSPs at the core NGCS nodes within the state of Nebraska.

Hamilton acknowledges that significant coordination and collaboration will be needed to successfully make the transition to NG 9-1-1 for the state of Nebraska. Working closely with existing OSPs in a manner that facilitates communication, collaboration, and teamwork toward shared goals and objective will ensure this transition is successful.

Lastly, Hamilton acknowledges its responsibility as the NG 9-1-1 service provider to create the legal agreements, configuration, and interfaces between the OSPs and other carriers and accomplish this transition in a timely manner. This expertise in carrier transition and subsequent coordination will be integrated into Hamilton's overall approach, which will maximize efficiency and minimize risk during the transition period.

NGCS 7	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 7.				

Any additional documentation can be inserted here

The analysis of ingress trunking can, and should, take place during the OSP conversion process. OSPs that will continue to deliver services in legacy TDM format will be serviced with an LNG and will need to be hard provisioned because of the limitations of their trunking technologies. OSPs that can hand-off traffic in a native SIP format will be able to accommodate much larger trunk counts than was previously feasible because a few mbps can accommodate hundreds of calls as G722 high definition calls are 128 kbps. For TDM based OSPs, the TDM to IP conversion at the edge of the OSPs network may be limited by TDM trunk capacities but will be sized appropriately to optimize 9-1-1 call throughput. After conversion from TDM to IP there are no limitations caused by bandwidth. Hamilton has the ability, and responsibility, to monitor and oversee ingress trunk utilization and will maintain appropriate levels of trunking from the OSPs to ensure service levels are met.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 8.				

Any additional documentation can be inserted here:

The legacy network gateway (LNG) included in Hamilton's solution will 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.

Hamilton's solution complies with NENA 08-003, which is based on the Internet Engineering Task Force (IETF) RFCs, such as SIP (RFC 3261), HELD (RFC 5985/6155), PIDF-LO (RFC 4119 and successive updates), and IETF ECRIT best practices documents and American National Standards Institute (ANSI) standards.

The emergency services routing proxy (ESRP) processes ingress calls received using session initiation protocol (SIP) signaling with location embedded in the PIDF-LO from i3 compliant carrier networks, from legacy carriers, or selective routers via the legacy network gateway/legacy selective router (LNG/LSRG) or from an upstream i3-compliant ESInet.

The HELD interface into the ESInet's Location Database (LDB) is leveraged by the LNG to retrieve PIDF-LO, either by value or reference, to be delivered to the PSAP within the SIP messaging. The HELD interface is also presented to the PSAP CPE to provide dereferencing services and/or provide location updates for wireless calls.

To overcome the problems of legacy ALI systems, NENA recommends the use of the Location Interwork Function, or LIF, within the Legacy Network Gateway, utilizing an internal location database with steering data as needed. This database is often referred to as an LDB, or Location Database (NENA-INF-008.2-2014). The LIF is a part of the LNG, although it can be physically separated.

A Location Database (LDB) serves as both a legacy ALI database and as a LIS in an i3 NG 9-1-1 environment and is included in this response to fully replace the existing ALI database and enable smooth transition to NG 9-1-1.

When legacy systems present ANI to the LNG, the LNG will utilize the LDB within the LIF to attach location to the call. The LNG issues a HELD query to the LDB, which will return a PIDF-LO adhering to the NENA CLDXF standard. Typically, the LNG will attach the location-by-reference URL into the SIP header allowing downstream elements (such as an ESRP or terminating PSAP CHE) to perform a dereference query over HELD to get location-by-value.

	.				

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 10.				

Any additional documentation can be inserted here:

The legacy network gateway (LNG) external interfaces included in Hamilton's proposed solution will comply with NENA-STA010.2-2016, requirements SLA 1-23, and other applicable standards and requirements.

In addition, Hamilton's solution supports time division multiplexing (TDM) from originating service providers (OSPs) as the standard ingress signaling configuration. Other signaling options, such as primary rate interface (PRI) and centralized automatic message accounting (CAMA), can be supported upon request.

Hamilton's LNG external interfaces complies with the following applicable NENA standards:

- RFC 2246 Transport Layer Security (TLS)
- SIP RFC 2327 Session Description Protocol (SDP)
- RFC 2976 SIP Info for digit transmission (#,*) and interworking DTMF
- RFC 3204 MIME Media Types for ISUP and QSIG (ISUP only supported)
- RFC 3261 SIP Basic
- RFC 3262 SIP PRACK
- RFC 3263 Locating SIP servers for DNS lookup SRV and A records
- RFC 3264 SDP Offer/Answer Model
- RFC 3265 SIP Subscribe/Notify
- RFC 3311 SIP Update
- RFC 3323 Privacy Header Field (partial support)

- RFC 3325 Asserted Identity
- RFC 3326 SIP Reason Header
- RFC 3372 SIP for Telephones (SIP-T)
- RFC 3398 ISUP/SIP Mapping
- RFC 3515 SIP REFER
- RFC 3578 ISUP Overlap Signaling to SIP
- RFC 3581 Symmetric Response Routing
- RFC 3666 SIP to PSTN Call Flows
- RFC 3711 SRTP (for SIP)
- RFC 3725 Third Party Call Control for SIP
- RFC 3764 ENUM for SIP Address of Record
- RFC 3891 SIP Replaces Header
- RFC 3892 SIP Referred-By Mechanism
- RFC 4028 SIP Session Timer
- RFC 4244 SIP History info (for call diversion)
- RFC 4412 Communications Resource Priority for SIP (partial support)
- RFC 4568 SDP Security Descriptions for Media Streams
- RFC 4904 SIP tgrp (trunk group) parameter
- RFC 5806 SIP Diversion Header (Dialogic® IMG 1010 Integrated Media Gateway)
- RFC 6140 Bulk SIP Registration

RFC 7433 SIP UUI Mechanism SIP 3xx Gateway Responses and 302 Initiate SIP Trunk Group IDs (OTG, DTG) SIP Coder Negotiation SIP Busy Out SIP P- Charge-Info Header ITU-T Q.1912.5 - SIP and ISUP Interworking (includes SIP-I) and Overlap signaling (SIP to SIP ISUP) SIP Mediation (SIP to SIP) SIP to SIP-I/SIP-T.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 11.				

Any additional documentation can be inserted here

Hamilton's proposed solution exceeds this requirement as it supports end-to-end RTT, as well as transcoding between RTT and TTY in either direction. This includes situations where a RTT call is routed to a PSAP which does not yet support RTT and the call must be converted to TTY. It also supports the situation where a caller is using a TTY and the call is routed to a PSAP that supports RTT. Transcoding is particularly challenging between RTT and TTY due to the protocol differences, and Hamilton's solution relies not only on various standards documents such as ITU V.18, RFC 5194, but also on over 25 years of experience in providing TTY-based Relay Services for people with hearing loss.

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.	Comply	Partially Comply X	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 12.				

Any additional documentation can be inserted here

Hamilton's LNG supports obtaining the callback number associated with any pseudo ANI (pANI) that does not include the callback number. This may require Hamilton to obtain the callback number from the wireless or VoIP provider, resulting in include additional recurring and non-recurring costs that are independent of the RFP. Hamilton agrees to take responsibility for any possible recurring or non-recurring costs associated with this requirement.

Hamilton can, and will, provide the Commission with a list of 9-1-1 calls that cannot be delivered to a PSAP, such as failed calls. The proposed LNG is capable of obtaining the following details:

- PSAP for call destination (if determinable)
- ANI/pANI
- Call Back (wireless/VoIP) Number
- Carrier (from which the call originated)
- Start time of call MM/DD/YYYY, hh.mm.ss.s TZ
- End time of call MM/DD/YYYY, hh.mm.ss.s TZ

Lists will be provided in a format that can be sorted based on carrier, PSAP, and county.

Further, to overcome the problems of legacy ALI systems, NENA recommends the use of the Location Interwork Function (LIF) within the Legacy Network Gateway, utilizing an internal location database with steering data as needed. This database is often referred to as an LDB, or Location Database (NENA-INF-008.2-2014). The LIF is a part of the LNG, although it can be physically separated.

A Location Database (LDB) serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment and is included in this response to fully replace the existing ALI database and enable smooth transition to NG9-1-1.

When legacy systems present pANI to the LNG, the LNG will utilize the LDB within the LIF to attach location to the call. The LNG issues a HELD query to the LDB, which will return a PIDF-LO adhering to the NENA CLDXF standard. The LDB, through the use of an ESME, maintains always on connections to the various Mobile Positioning Centers (MPC) and VoIP Positioning Centers (VPC). Steering data within the LDB directs a query to the appropriate MPC or VPC based on the pANI. The MPC or VPC will include the callback number in its response. The LDB attaches this callback number into its PIDF-LO response.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 13.				

Any additional documentation can be inserted here

The LNG functional element (FE) of Hamilton's proposed solution is capable of logging all significant events and 9-1-1 calls received and processed. Additionally, each call log shall contain all relevant parameters defined in Section 5.11.3 of NENA-STA010.2-2016.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 14.				

Any additional documentation can be inserted here

Hamilton LNG log files are capable of being extracted in near real-time and will be available in a format suitable for importing either into a spreadsheet or word-processing program.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 15.				

Any additional documentation can be inserted here

The LNG functional element (FE) included in the Hamilton solution achieves the resiliency and redundancy detailed in Section 1.1.7, Public Safety Grade Definition. The proposed ESInet achieves 99.999% availability and 24x7x365 for call processing, ensuring there is no single point of failure that will disrupt the ability to provide on-going call processing. All functions required for call processing are deployed in a highly available configuration and duplicated across core sites and LNGs. In the event of failure or degradation of service of a given FE or loss of a physical site, transactions or call traffic are diverted to available components. IP transport paths for critical service components are redundant and designed for multi-path IP packet delivery. Therefore, the failure of a given IP transport mechanism will not affect the overall service delivery. All components of the Hamilton solution are designed and configured for continuous operation.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 16.				

Any additional documentation can be inserted here

Hamilton has developed a specialized functional element (FE) appliance to support legacy star code transfers via a conversion to SIP messaging. This FE appliance is named HFA and is deployed throughout our service footprint. We also support the conversion of SIP transfer messaging to star codes for integration of NG PSAPs to legacy E9-1-1 networks.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 17.				

Any additional documentation can be inserted here

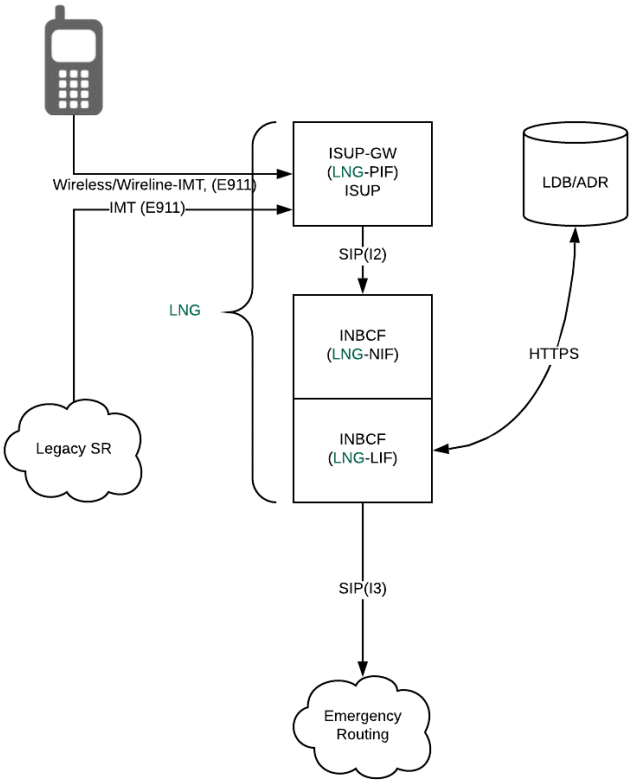
To fulfill the requirements of the contract, Hamilton, and its subcontractors, will be working from the following facility locations:

- Nebraska Data Center (NDC) – 1623 Farnam St., Omaha 68102
- Hamilton Data Center – 1006 12th St., Aurora, NE 68818

NDC is certified Tier 3 and Hamilton's data center is built to Tier 3 specifications that has been running at better than 99.999% uptime for over 10 years. NDC is operated by a separate entity, ensuring an additional layer of redundancy. Each data center has N+1 power redundancy.

The next generation core services (NGCS) cores will be located in the two data centers listed above. The NGCS cores will host the primary LNGs. The primary LNGs will facilitate the ingress of traffic from wireless providers as well as aggregated VoIP and CLEC traffic.

Additional LNGs will be located in datacenters, or negotiated carrier meet points, in each LATA within the state. These LNGs will primarily be used to ingress wireline traffic from the legacy LECs and Originating Service Providers. Traffic from the LNGs will be hauled to the NGCS core sites for routing to the destination.



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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 18.				

Any additional documentation can be inserted here

Hamilton accepts responsibility for meeting the timelines outlined above in both requirement NGCS 2 and NGCS 3. Both requirements address originating service provider (OSP) connectivity and Hamilton feels confident that its significant experience within the telecommunications industry can assist in its ability to meet, and exceed, all components of those two requirements. In addition, if the transition from the legacy selective routers to the next generation core services (NGCS) exceeds the committed timeline, and is attributable to the acts or omissions of Hamilton, Hamilton 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: Hamilton complies with requirement NGCS 19.				

Any additional documentation can be inserted here

Hamilton will provide and support Oracle 4600 series session border controllers (SBC). Oracle SBCs have been widely used in similar deployments and fully satisfy the requirement described above. The proposed solution includes firewalls, border control functions (BCF), and the implementation of access control lists (ACL) at all transitional ingress and egress interface points. The BCF functional elements will comply with all applicable standards including NENA STA-010.2-2016.

At the CPE handoff, an additional layer of security is included with the egress SBC (eBCF) functionality. All handoffs facing the PSAP or PSAP CPE host are required to interconnect at the SBC. This allows for a more secure handoff, plus additional session initiation protocol (SIP) message options to support non-NENA i3 interfaces, such as star codes or hook flashes, in conjunction with the legacy PSAP gateway (LPG).

The proposed solution utilizes the Fortinet intrusion prevention systems (IPS) within the BCF functional elements. Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

Telephony denial of service (TDoS) and distributed denial of service (DDoS) attacks can be difficult to identify, especially when originating from legacy originating service providers (OSP) and require a multi-threaded process to mitigate associated vulnerabilities.

Legacy network gateways (LNG) and SBCs are monitored with threshold detection to identify trunk saturation from the OSP network. Once alarmed, the network operations center/security operations center (NOC/SOC) will take action to identify the source, such as IP address, automatic number identification (ANI), or pseudo automatic number identification (pANI).

The proposed solution supports a network-based Conference/Transfer Function using the “Answer all-calls at a bridge” model identified by i3 and included in the proposed xBCF. This conference model does not require all calls consume Media Resources as the title may suggest (i.e. calls are only rehomed to Media Server Elements as needed when REFER is used). To accomplish a Conference or Transfer the Proposed Solution accepts REFER from Call Handling on any call

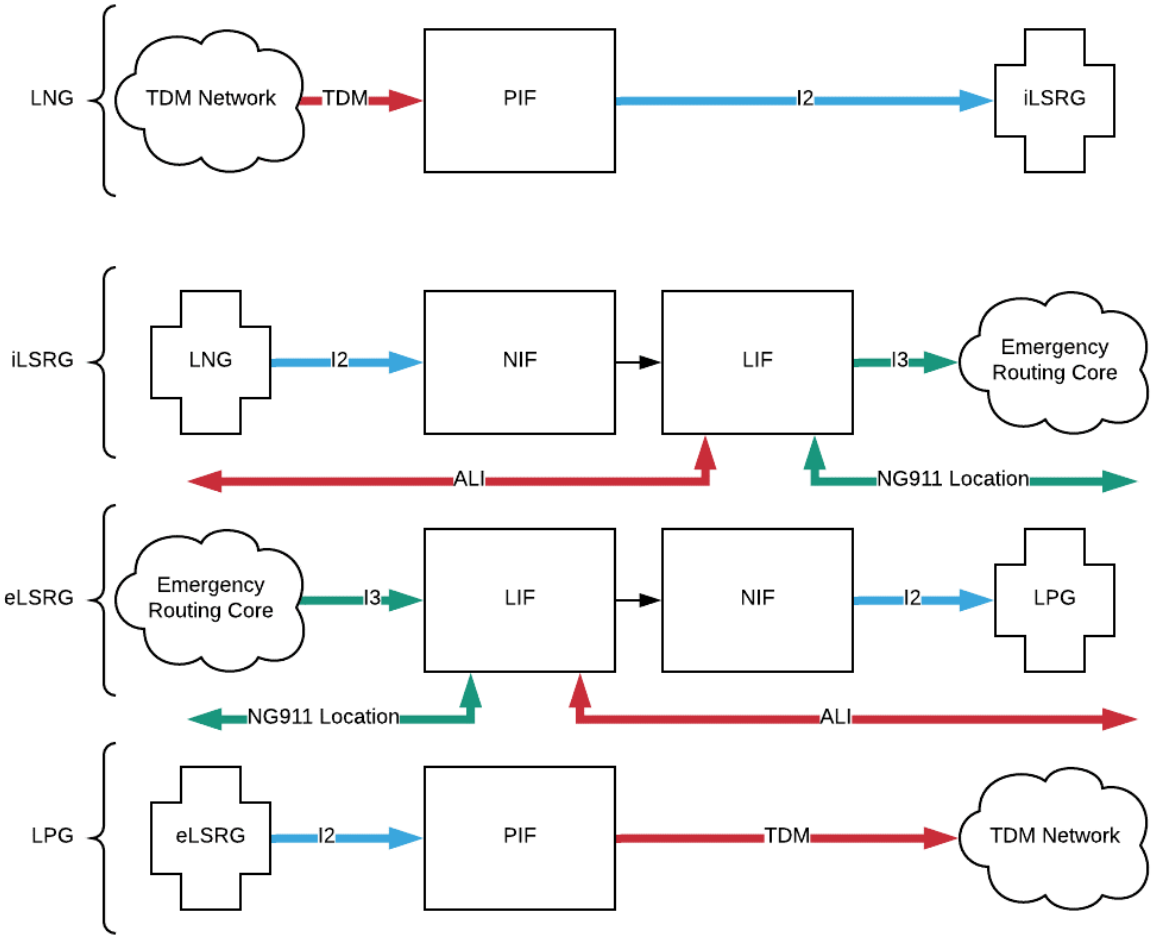
traversing the NGCS and by using Third Party Call Control w/re-INVITE offers a robust Network based Conference/Transfer Function.

This conference model provides for more efficiency and reliability around Conference/Transfer Function where invoking a conference is available to all calls and only calls needing media resources within the NGCS have assigned them. The proposed solution supports both MSML and Dialogic's XMS ReST API for Media Resource Function integration.

This functional element is compliant with, but not limited to, these RFCs:

- RFC-3261, SIP 2.0 Standard
- RFC-2327, SDP
- RFC-3264, Offer/Answer using SDP
- RFC-2246, TLS
- RFC-3265, SUBSCRIBE/NOTIFY
- RFC-4579(Section 5.5 and 5.11), Conference Aware Focus
- RFC-4575, Conference Event Package
- RFC-4028, SIP Session Timers
- RFC-4904, Trunk Groups in SIP
- RFC-5707, MSML (Media Server Markup Language) Note - only Voice is supported for Conference/Transfer when using MSML w/MRF (Media Resource Functions).

The following diagram has been included to more fully describe Hamilton's BCF functional element.



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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 20.				

Any additional documentation can be inserted here:

Hamilton's BCF solution will be deployed in a manner to achieve 99.999 percent availability.

The BCF solution is deployed in a fully active / active redundancy model. This allows a call to be routed to any active BCF instance in the event the original primary destination is unavailable. Each NGCS node is comprise of 2 "call chains" with redundant functional elements in each call chain. The nodes are configured to be redundant horizontally between nodes, as well as vertically within the node itself.

In addition to the in-market redundancy model, Hamilton also employs an N+1 model utilizing a national next generation core services (NGCS) infrastructure. The national infrastructure is designed to ensure that any call processing node is able to deliver a call in the event of a catastrophic in-market failure or a more likely scenario of a planned large-scale maintenance event.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 21.				

Any additional documentation can be inserted here:

Hamilton monitors and audits all aspects of the network for threats from a variety of sources. Packet level capture and forensics and net flow statistics are continuously monitored. This provides the capability to assist in troubleshooting and anomaly resolution, as well as providing assurance of reliable performance.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 22.				

Any additional documentation can be inserted here:

While our border control function (BCF) is capable of supporting silence suppression or comfort noise, we do not recommend that silence suppression or comfort noise be used in any VoIP deployment, especially NG 9-1-1. NG 9-1-1 calls should use G.711u or G.722 with no audio modifiers enabled. These low-quality compression concepts change the nature of the audio being transmitted and received and are known as problematic in this industry. Intentionally, these options are turned off in our media handling elements and we do not believe there is a need to preserve this function.

These options do not have a positive impact to VoIP calls. For example, while they may save a small amount of bandwidth, this is unpredictable and can throw off bandwidth calculations, etc. The primary concern includes losing valuable audio information at the time of the call, or in recordings, that mask forensic evidence post-call. This small amount of unreliable bandwidth savings is not worth the loss in audio quality.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 23.				

Any additional documentation can be inserted here:

In accordance with NENA-STA010.2-2016, the BCF included in Hamilton's proposed solution will mediate all incoming 9-1-1 calls from VoIP providers to SIP calls.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 24.				

Any additional documentation can be inserted here:

As specified in NENA-STA010.2-2016, the BCF included in Hamilton's proposed solution maintains logs of all 9-1-1 sessions and all additional BCF logging and recording requirements.

PSAP administrators can view end-to-end call detail records (CDRs) in real-time via a customer management portal. These CDRs include the start time of the call as it enters the ESInet, answer time, end time, digits for automatic number identification (ANI), and any errors encountered.

In addition, per NENA STA-010.2 specification, i3 logs from all ESInet i3 components will be available. Hamilton will support real-time log delivery and web service interfaces for log retrieval from authorized clients.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 25.				

Any additional documentation can be inserted here:

Hamilton's interconnection border control function (INBCF) product does not directly support network address translation (NAT) traversal. To resolve this, the mated SBC used with our BCF solution does offer a full NAT and network address and port translation (NAPT) supporting entrance point.

It is not Hamilton's recommendation to intentionally design networks with non-VoIP or IP-based multimedia services (IMS) aware firewalls. For this reason, SBCs are utilized to cross network boundaries where NAT is needed to eliminate the

need for "fixing up" protocols after a translation takes place. The problem of needing NAT traversal fixups can be eliminated when using the proper network functions in the call path

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 26.				

Any additional documentation can be inserted here:

The solution proposed by Hamilton will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards.

All proposed network equipment has the capability to utilize IPv4 and IPv6 and is configurable to support dual stack operation. Some internal systems solely support IPv4, however, this will not be a limitation for the solution proposed by Hamilton. For example, when an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet core will strip down the IPv6 packet, removing the IPv6 header, will add the IPv4 header, and will pass it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. Both the IPv4 network and the IPv6 interfaces are monitored continuously for availability and performance. This is accomplished with the use of a back-to-back user agent (B2BUA) session border controller (SBC), as compared to network address translations (NATs). All devices within the network will be assigned static addresses.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 27.				

Any additional documentation can be inserted here:

The selected SBC will support user datagram protocol (UDP), transmission control protocol (TCP), and stream control transmission protocol (SCTP) (model dependent) in SIP transport. Hamilton's functional elements support UDP and TCP; SCTP is currently on the roadmap.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 28.				

Any additional documentation can be inserted here:

The SBC will be capable of populating Layer 3 headers, based on call/session type, to facilitate priority routing of the packets. For example, on the egress, the combination of the SBC and BCF will support the ability to detect a call-type via embedded SIP details and apply DSC codes.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 29.				

Any additional documentation can be inserted here:
The solution proposed by Hamilton utilizes the Fortinet intrusion prevention systems (IPS) within the BCF functional elements (FE). Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

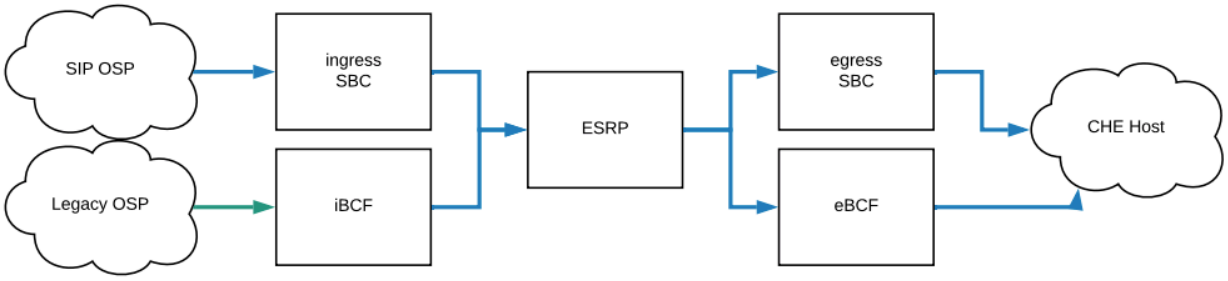
Telephony denial of service (TDoS) and distributed denial of service (DDoS) attacks can be difficult to identify, especially when originating from legacy originating service providers (OSP) and require a multi-threaded process to mitigate associated vulnerabilities.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 30.				

Any additional documentation can be inserted here:

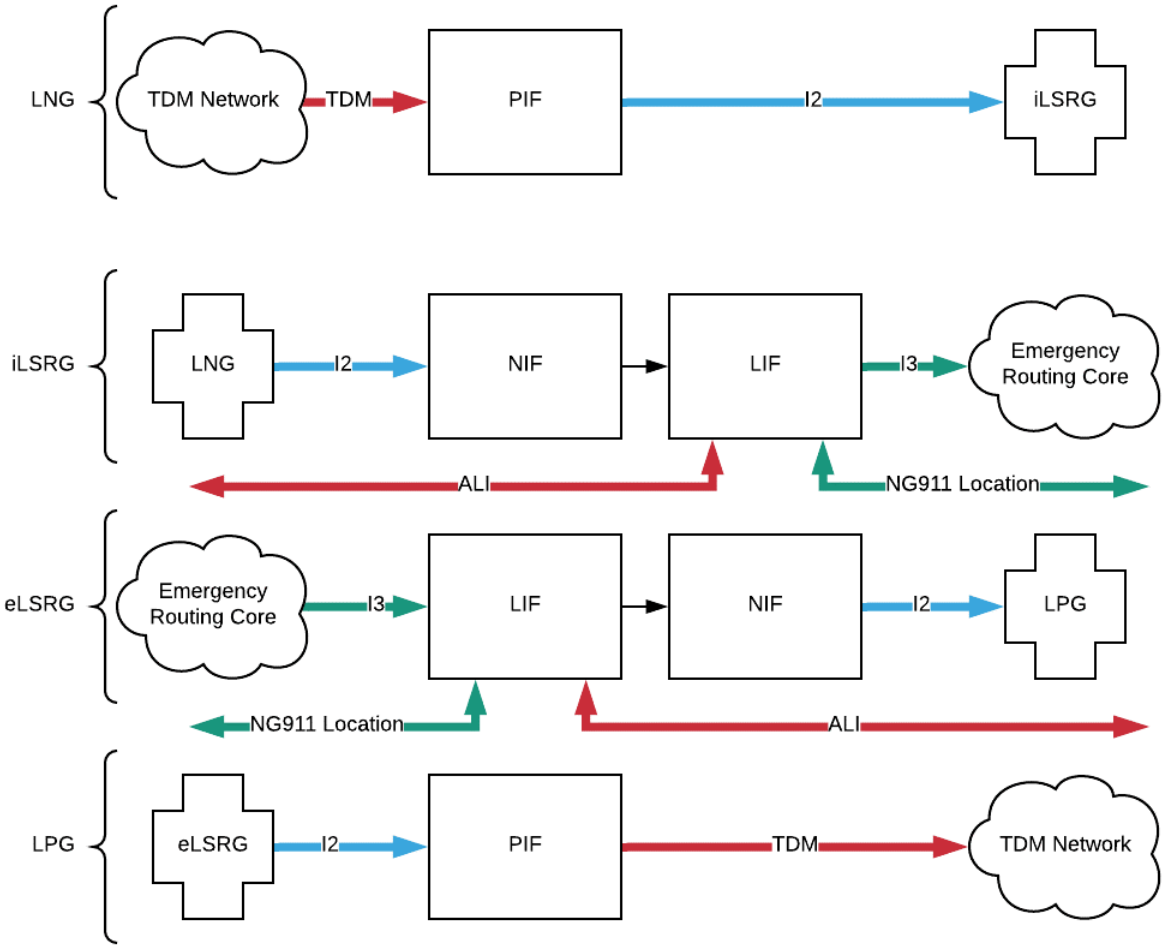
Border Control Function (BCF) Elements

Hamilton provides a border control function (BCF) on both the ingress (carrier facing) and egress (RCH/PSAP facing) sides of the ESRP. We refer to these as iBCF on the ingress side and eBCF on the egress side. Additionally, in the case of an OSP connecting with a native SIP interconnection to Hamilton, an Oracle SBC may be used to provide the BCF.



BCF Elements &/or Interfaces

The following diagrams depicts the different border control function (BCF) included in the proposed solution:



The solution proposed by Hamilton includes firewalls, border control functions (BCF), and the implementation of access control lists (ACL) at all transitional ingress and egress interface points. The BCF functional elements will comply with all applicable standards including NENA STA-010.2-2016.

At the CPE handoff, an additional layer of security is included with the egress SBC (eBCF) functionality. All handoffs facing the PSAP or PSAP CPE host are required to interconnect at the SBC. This allows for a more secure handoff, plus additional session initiation protocol (SIP) message options to support non-NENA i3 interfaces, such as star codes or hook flashes, in conjunction with the legacy PSAP gateway (LPG).

The proposed solution utilizes the Fortinet intrusion prevention systems (IPS) within the BCF functional elements. Fortinet IPS provides detection and survivability to egregious security attacks. These include zero-day, advanced targeted attacks, ransomware, polymorphic, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats. IPS, in combination with good network management techniques, like shutting down unused ports and services and configuring current access control lists (ACL), provides secure access to the ESInet.

Telephony denial of service (TDoS) and distributed denial of service (DDoS) attacks can be difficult to identify, especially when originating from legacy originating service providers (OSP) and require a multi-threaded process to mitigate associated vulnerabilities.

Legacy network gateways (LNG) and SBCs are monitored with threshold detection to identify trunk saturation from the OSP network. Once alarmed, the network operations center (NOC) will take action to identify the source, such as IP address, automatic number identification (ANI), or pseudo automatic number identification (pANI).

The proposed solution supports a network-based Conference/Transfer Function using the "Answer all-calls at a bridge" model identified by i3 and included in the proposed xBCF. This conference model does not require all calls consume Media Resources as the title may suggest (i.e. calls are only rehomed to Media Server Elements as needed when REFER is used). To accomplish a Conference or Transfer the Proposed Solution accepts REFER from Call Handling on any call traversing the NGCS and by using Third Party Call Control w/re-INVITE offers a robust Network based Conference/Transfer Function.

This conference model provides for more efficiency and reliability around Conference/Transfer Function where invoking a conference is available to all calls and only calls needing media resources within the NGCS have assigned them. The proposed solution supports both MSML and Dialogic's XMS ReST API for Media Resource Function integration.

This FE is compliant with, but not limited to, these RFCs:

- RFC-3261, SIP 2.0 Standard
- RFC-2327, SDP
- RFC-3264, Offer/Answer using SDP
- RFC-2246, TLS
- RFC-3265, SUBSCRIBE/NOTIFY
- RFC-4579(Section 5.5 and 5.11), Conference Aware Focus
- RFC-4575, Conference Event Package
- RFC-4028, SIP Session Timers
- RFC-4904, Trunk Groups in SIP
- RFC-5707, MSML (Media Server Markup Language) Note - only Voice is supported for Conference/Transfer when using MSML w/MRF (Media Resource Functions).

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 31.				

Any additional documentation can be inserted here:

Hamilton's proposed solution includes an emergency service routing proxy (ESRP) that complies with all tested NENA standards, including NENA-STA-010.2-2016. This functional element (FE) has been tested at multiple NENA ICE events and field proven in multiple statewide deployments.

ESRPs are deployed as geo-redundant systems in an active / active configuration. Deployment makes use of virtual server environments to provide multiple instances of the ESRP application to exceed 99.999% availability.

In the call flow progression, the ESRP makes a routing decision based upon location. On nomadic based calls, the location information service (LIS) will query third party location providers via E2+ links.

As location is added to SIP messaging by the originating service providers (OSP) or is available from wireline records that have been location validation function (LVF) validated, the ESRP queries the emergency call routing function (ECRF) for a routing destination. The ESRP then routes the call to the proper PSAP with a destination ID or a pre-routed SIP identifier to the CPE.

The policy routing function (PRF) is an integral part of the NGCS system and is the component that enables 99.999% availability. The PRF provides alternate routing procedures for call routing in the event of failures in the call flow. PRF can be unique to each PSAP, but for the purposes of this response, the most common deployment technique will be illustrated.

The PRF follows a prioritized decision tree after routing to determine where to ultimately deliver the emergency call. Typically, calls are delivered to the named queue selected by geo-routing's next-hop uniform resource identifier (URI). When alternate treatment is required, Hamilton's NOC/SOC is available to meet the customized needs of the PSAP. This ensures that the operation of the network remains compliant with ICC regulations, and that all changes are thoroughly tested after implementation.

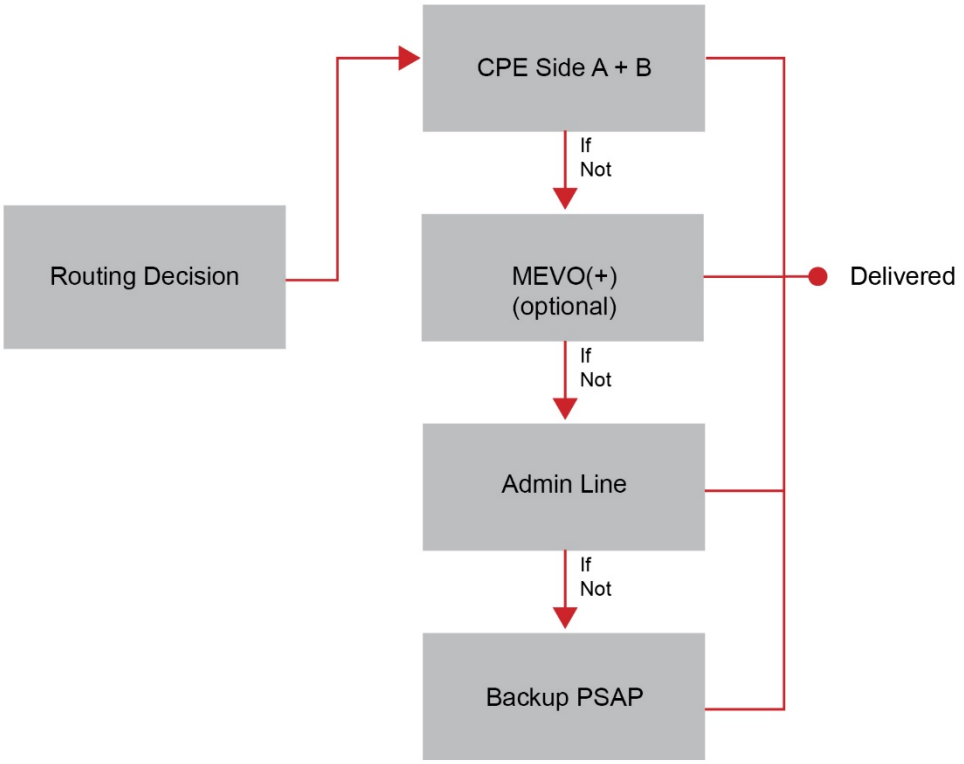
There is no limitation on how many destinations can be added to the PRF. The PRF also includes unanswered call timers as well. Once a timer has expired, the call is attempted to be delivered to the next resource. A resource in the decision tree that responds with a status of unavailable causes the PRF logic to advance to the next available resource.

The PRF/ESRP also behaves differently depending on SIP rejection messages presented by the next device in the call flow, providing a "look ahead" function. This saves critical time in call routing.

Another critical aspect of call flow is network redundancy and failover. The data centers will be connected via redundant high capacity links from two different providers. Additionally, a third connection will be created via a 4G / 5G / FirstNet connection, utilizing a VPN to maintain security, to sustain connectivity in the event of primary network failure.

This FE is compliant with, but not limited to, these RFCs:

- RFC-3261, SIP 2.0 Standard
- RFC-2327, SDP
- RFC-3264, Offer/Answer using SDP
- RFC-2246, TLS
- RFC-3265, SUBSCRIBE/NOTIFY
- RFC-4579(Section 5.5 and 5.11), Conference Aware Focus
- RFC-4575, Conference Event Package
- RFC-4028, SIP Session Timers
- RFC-4904, Trunk Groups in SIP
- RFC-5222, LoST
- RFC-5985, RFC-6753, HELD
- RFC-6848, RFC-4119, RFC-4479, RFC-5139, RFC-5491, NG911 Location, a.k.a. PIDF-Lo
- RFC-4848, U-NAPTR DDDS
- RFC-6442, Location Conveyance



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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 32.				

Any additional documentation can be inserted here:

Hamilton's subcontractor, GeoComm, is providing the emergency call routing function (ECRF) which supports either legacy fields or i3 compliant fields based in CLDXF. The GeoComm ECRF can be ready to provide geospatial routing information at initial cutover. In addition, GeoComm currently manages GIS data for the majority of Nebraska counties and regions.

The MSAG Conversion Service (MCS) supports legacy CPE and the database (LDB) in the transition of records from MSAG based address to PIDF-LO by using the GIS data. MCS is a web service defined by NENA for the transition from legacy to i3 systems.

GIS MSAG Delta services include one-time services to build a GIS derived MSAG, as well as MSAG delta processing services to assist the State with maintaining ongoing synchronization between the State's NG 9-1-1 Road Centerline layer and the aforementioned GIS derived MSAG used by the LDB.

The pricing for the MSAG Conversion Service (MCS) and LDB is a stand-alone monthly recurring cost (MRC) for each region. As the regions are converted to geospatial routing, the MSAG Conversion Service (MCS) and LDB function is no longer needed. As a result, the MRC for the LDB/MCS service will decrease over time until being completely removed from service.

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: Hamilton complies with requirement NGCS 33.				

Any additional documentation can be inserted here:

Using the location determined uniform resource identifier (URI), from the emergency call routing function (ECRF) via the LoST protocol, the ESRP interacts with the policy routing function (PRF) to determine call routing.

The PRF accounts for the operational status of any downstream ESRP in the evaluation of any policy, ensuring that an ESRP is in an operational state prior to any messages being sent to that ESRP's queue.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 34.				

Any additional documentation can be inserted here:

Hamilton is tracking the adoption pace of these extended i3 concepts, with the goal of producing an immediately usable set of quality, reliable products.

As STA-010 matures, all identified Conditions and Actions will be supported in future releases. Currently, the policy routing function (PRF) handles the following focused set of Conditions and Actions taken from STA-010 and operational experience:

- Service, Element and Queue State Conditions
- Time of Day Condition
- Dialed Number Condition (a.k.a. DNIS)
- Route Action

Currently, the PRF queue is defined as a static assignment to a dequeuer URI, not currently utilizing deQueue registration or needing SUBSCRIBE/NOTIFY to reliably deliver calls. That being said, Hamilton's next generation core services (NGCS) solution will fully support deQueue Web-service and appropriate SUBSCRIBE/NOTIFY event package(s) in an upcoming release. SUBSCRIBE/NOTIFY is in quality assurance (QA) at the time of this writing.

Hamilton's emergency service routing proxy's (ESRP) deQueue functionality has been tested and qualified as proof-of-concept work. It has been met with somewhat fragmented support from our CPE partners, who are not at the same stage of support for this set of features.

We are balancing the need to focus our resources on the higher priorities that are related to the requirements of transitional networks as they relate to emerging NG 9-1-1 projects. As the i3 deQueue mechanism becomes valuable or widely adopted, Hamilton will be ready to support it.

The policy store is currently restricted internally to the NGCS functional elements (FE) only; this does come with an API and graphical tool for manipulation. It is on the roadmap to support an external Policy Store once the standard has matured and third-party vendors support emerges.

		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: Hamilton complies with requirement NGCS 35.				

Any additional documentation can be inserted here:

Hamilton's next generation core services (NGCS) ingress emergency services routing proxy (INESRP) supports the i3v2 defined model for Queues. The ECRF LoST findService's response (e.g. after Georouting function), if successful, will indicate a next-hop URI. This next-hop URI is matched up to a provisioned i3 Queue for policy routing function (PRF) processing, with a likely result of subsequent delivery to the next-hop beyond the local ESRP. For example, the egress border control function (EBCF) or CHE functional elements.

This next-hop URI, when pointing to a provisioned i3 Queue, is initially used as an identifier to start the associated agency's policy routing rules (PRR) decision tree and session delivery logic. This same URI can subsequently be re-used as a "de-queuer" URI in a statically configured Endpoint, Dynamic Dequeue Registration, or later as a URI in a Route rule to identify the next-hop beyond the ESRP. This way, the normal next-hop URIs within GIS layers can be used within the ESInet's SIP realm without conflict. INESRP's Endpoint and derived Element State model defines using SIP awareness of predefined UAs within PRF, where rules, synthesized states and logic can fulfill the desire of an Agency with special needs to build a specific strategy to receive emergency eessions.

These PRF rules, as assigned to the next-hop URI, can take into account multiple i3 State(s), time and date, along with other operational details and knowledge of the emergency call or caller to identify how and where SIP sessions are delivered to. Endpoints are used by INESRP to interoperate with SIP-only downstream elements using SIP OPTIONS. SIP SUBSCRIBE is also supported for any i3 supporting functional elements exposed by the terminating ESInet for SIP session delivery.

Please note, that as of this writing, Dequeue Registration is a manual process called "Endpoints." However, it is on the INESRP roadmap to fully support both web service and SIP REGISTER models for dynamic queues as they become operationally viable in an identified peering CHE solution. In the interim, i3 queues are pre-defined within the INESRP configuration and rules, applied by CraftsPerson, occur over a secure API using provided provisioning tools.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 36.				

Any additional documentation can be inserted here:

The redundant and resilient ESRP/PRF solution proposed by Hamilton will provide a minimum of 99.999 percent availability. In addition, Hamilton maintains at least two backup copies of the policy rules at geographically diverse sites, depending on the requirements of the project. Hamilton will maintain back-up copies at its datacenter locations, Omaha, NE, and Aurora, NE. If needed, additional backup copies can be maintained at Hamilton's other data center locations

Additionally, this functional element is compliant with, but not limited to, these RFCs:

- RFC-3261, SIP 2.0 Standard
- RFC-2327, SDP
- RFC-3264, Offer/Answer using SDP
- RFC-2246, TLS
- RFC-3265, SUBSCRIBE/NOTIFY
- RFC-4579 (Section 5.5 and 5.11), Conference Aware Focus
- RFC-4575, Conference Event Package
- RFC-4028, SIP Session Timers
- RFC-4904, Trunk Groups in SIP
- RFC-5222, LoST
- RFC-5985, RFC-6753, HELD
- RFC-6848, RFC-4119, RFC-4479, RFC-5139, RFC-5491, NG911 Location, a.k.a. PIDF-Lo
- RFC-4848, U-NAPTR DDDS
- RFC-6442, Location Conveyance

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 37.				

Any additional documentation can be inserted here:

Hamilton's next generation core services (NGCS) ingress emergency services routing proxy (INESRP) creates a derived element state that can be used for decision making within policy routing function (PRF) logic. Within i3, an "element State" holds the status of a downstream functional element. The INESRP will create a synthesized element state by using the SIP OPTIONS message per configured endpoint(s) to determine true SIP availability.

An endpoint is an INESRP configured awareness for a specific SIP UA that defines a static SIP transport identity for a next hop of a queue as a point reachable by a route rule. The route rule will contain a URI that ultimately lives at or beyond a next hop SIP endpoint. The endpoint identifies the SIP UA's host configuration to be associated with one or more SIP next hop URI(s). The endpoint's settings and perceived availability will match up to the SIP UA or host as a result of the OPTIONS message responses.

The Endpoint configuration is used by INESRP's internal logic and resultant element state is available within PRF rules as used

within multiple queues' configuration. The SIP hosts used for URIs assigned by egress route rules can be probed using this endpoint model to support a derived element state for each. The element state can be used by any policy routing rule (PRR) to determine the "synthesized" availability of the downstream UA based on OPTIONS probing of the associated endpoint.

To start using this SIP OPTIONS functionality, an endpoint is created identifying the transport details of the SIP UA (e.g. TCP Address and Port, and the parameters of the OPTIONS probing). INESRP will start to probe the UA and update the identified element state to reflect the perceived availability of the identified UA. Both PRR's route and state rules can be used with this endpoint/element combination to ensure the next hop's state prior to attempting to dequeue an emergency session to it.

Hamilton's NGCS INESRP fully supports the i3 SUBSCRIBE/NOTIFY model to determine the status of next hop queue service or element. These actual i3 states can be used alongside the derived states, as described for element, and both can be used within PRF rules without conflict.

	Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF TCP/TLS Implementation	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 38	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: Hamilton complies with requirement NGCS 38.				

Any additional documentation can be inserted here:

The ESRP fully supports the requirements of STA-010 regarding the use of Transmission Control Protocol/Transmission Layer Security (TCP/TLS) and UDP for the transport of SIP. The ESRP fully supports the use of the emerging PSAP Credentialing Authority (PCA) as defined by NENA for certificate management and validation.

Based on the documentation provided below, acceptance criteria will be taken from development artifacts. The ESRP will use TLS if configured first, TCP next, with eventual fallback to UDP. This is supported for any configured or registered SIP endpoint.

The ESRP can be configured with a Certificate for when it is a server, as in receiving TLS requests, and with a managed trusted root certificate store when acting as a client; both perspectives are needed for mutual authentication and full SIP TLS support.

Acceptance Criteria

- If TLS transport fails or is not available, SIP elements SHOULD attempt to use TCP.
- If TLS and TCP transports both fail or are unavailable, SIP elements SHOULD fall back to UDP transport.
- Non-SIP communications will not need to include previous points.

Description

- This is motivated by STA-010.3 i3 Standard Pub Rev published in June 17th, 2019.

3.1.2.12 Transport

- All SIP elements must support TLS, TCP, and UDP transport. SIP signaling within the ESInet should be carried with TLS. If TLS transport fails or is not available, SIP elements should attempt to use TCP. If TLS and TCP transports both fail, or are unavailable, SIP elements should fall back to UDP transport.
- This change only would make sense in SIP call routing (excluding ECRF and LIS resolution).

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.				
	Bidder Response: Hamilton complies with requirement NGCS 39.				

Any additional documentation can be inserted here:

Hamilton's emergency service routing proxy (ESRP) complies with all known NENA standards, including STA-010.2-2016 and the functional requirements listed below as part of the NENA Compliance Chart. This functional element has been tested at multiple NENA ICE events and field proven in multiple statewide deployments.

	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: Hamilton complies with requirement NGCS 40.				

Any additional documentation can be inserted here:

The GeoComm emergency call routing function (ECRF) is designed and tested to support recursive queries within an ECRF hierarchy. This will allow for interoperability with neighboring states, sub state level regions that choose to operate their own ECRF, ECRF/Forest Guide operated by a local or regional Originating Service Provider (OSP) or a national Forest Guide.

NGCS 41	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 41.				

Any additional documentation can be inserted here:

The GeoComm emergency call routing function (ECRF) and location validation function (LVF):

- Provide fast, secure, and reliable core network ECRF services for NG 9-1-1.
- Enable fast geo-spatial 9-1-1 call routing and location based selective transfers.
- Provide industry standard i3 location validation.
- Include and ad-hoc routing boundary editor.
- Include a Network Operations Center (NOC) dashboard, and monitoring and reporting capabilities.
- Were tested for interoperability at NENA ICE 1-8, and EENA/ETSI Plugtest #1.
- Support NG 9-1-1 additional data discovery.
- Accept NENA i3 standardized Spatial Interface (SI feeds) for ingesting GIS updates.
- Contain a dashboard suitable for display in a NOC.
- Support NENA i3 logging, Simple Network Management Protocol (SNMP), as well as raw log data outputs for third party monitoring and logging solutions.

The ECRF and LVF solution is designed for flexibility, consistency, security, and scalability. It consists of four high-level components:

- ECRF and LVF Web Service: the engine that services Location to Service Translation (LoST) queries
- GIS Database: centralized, highly available source of GIS data for servicing LoST queries
- Provisioning: services for loading and updating GIS data from GIS Data Hub into the GIS database
- Dashboard and Ad-hoc Routing Web Applications: web applications for monitoring system health and creating ad-hoc routing boundaries

GIS Data is provisioned in one of two ways:

1. Bulk load of a full GIS dataset from GIS Data Hub, or,
2. Incremental update provisioning through the NG 9-1-1 GIS data management SI Feed

Generally, bulk loads would occur during the initial system set up and incremental update provisioning would occur after cutover. Regardless of the method, provisioning is performed without interruption to the ECRF and LVF Web Services running in the same cluster and is coordinated to ensure data is consistent across clusters.

NGCS 42	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 42.				

Any additional documentation can be inserted here:

GeoComm ECRF's architecture is a load balanced, fault tolerant system of GIS servers, database servers, and web servers deployed using docker containers and Kubernetes, with no single point of failure, and is capable of 99.999% uptime when deployed across multiple data centers. To meet the 99.999% up time requirement, the system is designed with N+1 capacity and redundancy on all tiers. The system is designed to handle 50k requests per hour even during a maintenance event or a component failure.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 43.				

Any additional documentation can be inserted here:

GeoComm provides an external instance that handles external ECRF requests and LVF requests.

GeoComm ECRF responds to LoST queries defined in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5222, established in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards for the NENA i3 Solution. To discover a service URI for a particular location, the LoST protocol specifies a <findService> request. GeoComm ECRF responds to <findService> requests as well as other LoST protocol requests. GeoComm ECRF is provisioned with the changes to the GIS dataset supplied by GeoComm SI. Authorized i3 functional elements, such as an NG 9-1-1 ESRP, may query GeoComm ECRF with a geodetic or civic location and a service URN describing the type of service requested, in a LoST <findService> request. GeoComm ECRF queries the GIS database that has been provisioned to discover and return a service URI, which is used by the ESRP to send the call to the correct next hop destination.

While GeoComm ECRF may technically be accessed both from inside and outside the ESInet, for security purposes it is not recommended that the same ECRF cluster is accessible both inside and outside the ESInet. If the State requires an ECRF which is accessible outside of the ESInet, it is recommended a separate ECRF cluster is deployed. It is further recommended that the ECRF outside the ESInet be deployed at a later date after the overall structure of the relationship(s) with the originating service provider(s) is established.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 44.				

Any additional documentation can be inserted here:

The GeoComm ECRF can be queried by any entity authorized to connect the ESInet and is fully compliant with all standard call types.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 45.				

Any additional documentation can be inserted here:

An origination network may query the external ECRF provided with the system, use its own forest guide or use the national forest guide.

In the event an OSP would like GIS call routing data in their own solution, they would be able to use the supplied NENA i3 compliant SI to update GIS data within their network.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 46.				

Any additional documentation can be inserted here:

GeoComms ECRF is compliant to NENA standards and allows queries from any authorized source such as the emergency service routing proxy (ESRP), legacy network gateway (LNG), border control function (BCF), PSAP systems, call handling equipment and more.

Additionally, an external ECRF instance is provided outside of the call routing network to allow authorized external sources to query the systems authoritative ECRF. This can be used for interaction with neighboring states, adjoining PSAPs, OSPs, or use with the forest guild.

GeoComm ECRF supports responding to iterative and recursive LoST queries, as detailed in RFC 5222.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 47.				

Any additional documentation can be inserted here:

GeoComm ECRF is an IETF 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF as specified in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards. There are many related Request for Comments (RFC) that define how GeoComm ECRF operates, including PIDF-LO, RFC 4119 and its revision RFC 5139.

GeoComm ECRF responds to LoST queries defined in IETF RFC 5222, as specified in NENA-STA-010.2-2016. To discover a service URI for a particular location, the LoST protocol specifies a <findService> request. GeoComm ECRF responds to <findService> requests as well as other LoST protocol requests. GeoComm ECRF is provisioned with the aggregated GIS dataset supplied by the State. Authorized i3 functional elements, such as an NG 9-1-1 ESRP, may query the ECRF with a geodetic or civic location and a service URN describing the type of service requested, in a LoST <findService> request. The ECRF queries the GIS database that has been provisioned to it in order to discover and return a service URI, which is used by the ESRP to send the call to the correct next hop destination.

		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: Hamilton complies with requirement NGCS 48.				

Any additional documentation can be inserted here:

GeoComm ECRF may be configured in such a way to rate-limit queries. GeoComm ECRF queries are sent to a URL with high priority. All other queries (with a source other than the ESRP or other authorized LoST client) are sent to a different URL with a lower priority.

GeoComm ECRF has several logging mechanisms to facilitate transaction auditing, debugging, and activity monitoring. Diagnostic logs exist for all servers in the system, tracking any internal server errors that occur, which can then be analyzed for configuration and server errors. All LoST transactions are logged as well for a complete archive of activity. In addition, the logging mechanisms include i3 compliant log event reporting, meaning that within an ESInet, the ECRF can send request/response logs to an i3 compliant logging service. Finally, GeoComm ECRF includes a browser-based dashboard that shows current activity, generates transaction reports, and views the logs directly.

GeoComm's compliance with this requirement is predicated on the interpretation of "connection attempts" defined as connection attempts which hit the ECRF load balancer only. Logging any other connection attempts is not a function of GeoComm's solution.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 49	**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:				
	Bidder Response: Hamilton complies with requirement NGCS 49.	X			

Any additional documentation can be inserted here:

GeoComm ECRF has several logging mechanisms to facilitate transaction auditing, debugging, and activity monitoring. Diagnostic logs exist for all servers in the system, tracking any internal server errors that occur, which can then be analyzed for configuration and server errors. All LoST transactions passing through the ECRF are also logged, for a complete archive of activity. As part of the Spatial Interface (SI) proposed to the State, GIS data updates will include QA/QC measures performed on the statewide dataset aggregated by the State. This will include reporting to outline update start time, completion time, update outcome, etc.

Connection and connection attempt logging may be enabled by a network technician for trouble shooting. Connection and connection attempts logging are disabled by default.

Location error identification

GeoComm ECRF is highly configurable for routing locations that fall into a gap or overlap beyond using a default route. A buffer tolerance is set that allows for a gap or overlap to not return a default route. If the input is a point, reference the multiple match policy to identify the error. The policy would be either Return First, Return Limit Warning, or Return Error.

In the case of Return Limit Warning, there is an additional configuration value which dictates the maximum number of results to return. If there are more results to return than the established threshold, the response will include a warning. The default response warning is Return First.

If the input is a polygon, a user may reference the polygon multiple match policy to identify the error. The policy would be either Return First, Return Area Majority, or Return Error. In the case of Return Area Majority, there is an additional configuration value which indicates the maximum number of results to return. If there are more results to return than the established threshold, the response will include a warning. The default response warning is Return Area Majority with results listed in order of largest overlap to smallest.

Updates from the SI in near real-time with no degradation of LoST services

GeoComm ECRF and LVF both connect to a NENA compliant Spatial Interface (SI) and accept transactional updates without any disruption of services. GeoComm GIS Data Hub takes care of the GIS User interface that manages the QC process; once data passes QC checks, it is provisioned into the SI. Updates typivally move from the SI in the live ECRF call routing data within 30 seconds. GeoComm also provides a bulk load option for both ECRF and LVF that does not impact service availability.

Routing of calls based on geographic coordinates, geodetic shapes, and civic addresses

GeoComm ECRF can provide route mappings for geodetic location profiles as well as civic location profiles. Geodetic (coordinate based) locations may be point, polygon, circle, ellipse, or arc-band. Civic locations are street addresses including house number, street name, city name, etc.

GeoComm ECRF also implements a “best efforts” scheme in the event a civic location provided in a LosT <findService> request does not completely match GIS data that has been provisioned to the ECRF. For example, with a civic location containing an unrecognized street name, but valid city and state, the ECRF can return a service URI based on a PSAP service area boundary polygon wholly containing the civic location’s city. In this case, the <findServiceResponse> returned from the ECRF will also contain a <defaultMappingReturned> warning, indicating to the querying function that a default mapping was determining the route. An ESRP/CTI solution may display warning condition to a call taker when the <findServiceResponse> sent from the ECRF to the ESRP contains a <defaultMappingReturned> warning. This feature in GeoComm ECRF is a configurable option that may be turned on or off as a matter of policy. An alternative approach is for a CTI application to invoke LVF on every received call. If any part of a proffered civic location fails LVF, the call taker may be notified by the CTI application that the location is suspect.

Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS)

There is no limit to the number of GIS boundaries GeoComm ECRF is capable of consuming. However, as a matter of practicality, it is recommended the ECRF utilize the common GIS boundaries listed above (PSAP, law enforcement, fire, and EMS).

Permitting of LoST queries for find service request association with each layer

GeoComm ECRF responds to LoST queries defined in IETF RFC 5222, as specified in NENA 08-003. To discover a service URI for a particular location, the LoST protocol specifies a <findService> request. The ECRF responds to <findService> requests as well as other LoST protocol requests. GeoComm ECRF is provisioned with the aggregated GIS dataset supplied by the State. Authorized i3 functional elements, such as an NG9-1-1 ESRP, may query the GeoComm ECRF with a geodetic or civic location and a service URN describing the type of service requested, in a LoST <findService> request. GeoComm ECRF queries the GIS database that has been provisioned to it in order to discover and return a service URI, which is used by the ESRP to send the call to the correct next hop destination.

Compliance with NENA 02-010 and NENA 02-014

GeoComm ECRF complies with industry GIS standards, including NENA 02-010V9 and NENA 02-014v1.

Dynamic updates to GIS without disruption of the ECRF

GeoComm ECRF and LVF both connect to a NENA compliant Spatial Interface (SI) and accept transactional updates without any disruption of services. GeoComm GIS Data Hub takes care of the GIS User interface that manages the QC process; once

data passes QC checks, it is provisioned into the SI. Updates typically move from the SI in the live ECRF call routing data within 30 seconds. GeoComm also provides a bulk load option for both ECRF and LVF that does not impact service availability.

Validation of GIS updates before they are provisioned into the ECRF

GeoComm ECRF and LVF both connect to a NENA compliant Spatial Interface (SI) and accept transactional updates without any disruption of services. GeoComm GIS Data Hub takes care of the GIS User interface that manages the QC process; once data passes QC checks, it is provisioned into the SI. Updates typically move from the SI in the live ECRF call routing data within 30 seconds. GeoComm also provides a bulk load option for both ECRF and LVF that does not impact service availability.

	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	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 50	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.	X			
	Bidder Response: Hamilton complies with requirement NGCS 50.				

Any additional documentation can be inserted here:

1. Provisioning the ECRF;
2. Updating the ECRF (including the frequency of updates);
3. Validating data provisioning;

ECRF and LVF System Architecture and GIS Data Provisioning

The ECRF and LVF solution is designed for flexibility, consistency, security, and scalability. It consists of four high-level components:

- ECRF and LVF Web Service: the engine that services LoST (Location to Service Translation) queries
- GIS Database: centralized, highly available source of GIS data for servicing LoST queries

- Provisioning: services for loading and updating GIS data from GeoComm SI into the GIS database
- Dashboard and Ad-hoc Routing Web Applications: web applications for monitoring system health and creating ad-hoc routing boundaries

GIS data is provisioned in one of two ways. This may include either a bulk load of a full GIS dataset from the GeoComm Spatial Interface (SI) or an incremental update provisioning through the NG 9-1-1 GIS data management SI feed.

Generally, bulk loads would occur during the initial system set up and incremental update provisioning would occur after cutover. Regardless of the method, provisioning is performed without interruption to the ECRF and LVF Web Services running in the same cluster and is coordinated to ensure data is consistent across clusters.

Using the SI allows updates to flow directly from GIS Data Hub into the ECRF.

GeoComm SI allows the subscribed element such as GeoComm ECRF to acknowledge receipt of each transaction. Then, if the ECRF components detect an issue, it can use the GeoComm bulk load mechanism to repopulate a layer or the entire GIS database without service disruption.

4. Performing error logging;

Provisioning Errors

If errors are detected during the provisioning processes and a NENA compliant Discrepancy Report is created, details on the error are available in the GeoComm ECRF Operations Suite. Actions taken by the GeoComm ECRF are based on the type of error encountered.

Error Handling and Logging

GeoComm ECRF can capture unhandled exceptions and still return a response to the requestor indicating an internal error occurred. In addition, several other potential error conditions are checked for and reported back to the requestor including:

- Malformed XML or LoST syntax (bad request errors)
- Requested service URN is not supported (service not implemented errors)
- Invalid GML or coordinate values (location invalid errors)
- Unknown location profiles (location profile unrecognized errors)
- Spatial reference problems (SRS invalid errors)
- Revisiting an already queried server (loop errors)
- Recursive time out conditions (server timeout errors)
- Bad response from a recursively queried server (server errors)
- Access denied to recursively queried server (forbidden errors)

GeoComm ECRF has several logging mechanisms to facilitate transaction auditing, debugging, and activity monitoring. Diagnostic logs exist for all servers in the system, tracking any internal server errors that occur, which can then be analyzed for configuration and server errors. In addition, all LoST transactions are logged for a complete archive of activity. Logging mechanisms also include i3-compliant log event reporting. This means that, within an ESInet, the servers can send ECRF request/response logs to an i3 compliant logging service. Finally, the ECRF includes a browser-based dashboard which shows current activity and server status, generates transaction reports, and views the logs directly.

Integrated Logging

GeoComm ECRF has several logging mechanisms to facilitate transaction auditing, debugging, and activity monitoring. Diagnostic logs exist for all servers in the system, tracking any internal server errors that occur, which can then be analyzed for configuration and server errors. All LoST transactions passing through the ECRF are also logged, for a complete archive of activity.

In addition, the ECRF logging mechanisms include i3 compliant log event reporting, meaning that within an ESInet, the ECRF can send ECRF request/response logs to an i3 compliant logging service. Finally, the ECRF includes a browser-based dashboard that shows current activity and server status, generates transaction reports, and views the logs directly.

5. Performing gap and overlap analysis;

Performing gap and overlap analysis

GeoComm SI validates GIS database changes before they are sent to the live ECRF databases. Specifically, the system checks for gaps and overlaps in boundary polygons, road centerline layers crossing boundary polygon borders, attribute fields containing values outside of acceptable values, invalid geometries, and values missing from critical fields. These checks prevent invalid data from being provisioned to ECRF.

6. Supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet.

Query Support

GeoComm ECRF is an Internet Engineering Task Force (IETF) 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF as specified in specified in NENA-STA-010.2. There are many related Request for Comments (RFC) that define how GeoComm ECRF operates, including PIDF-LO, RFC 4119 and its revision RFC 5139. GeoComms ECRF allows queries from any authorized source such as ESRP, LNG, BCF, PASP systems, call handling equipment and more.

GeoComm ECRF responds to LoST queries defined in IETF RFC 5222, as specified in NENA-STA-010.2 To discover a service URI for a particular location, the LoST protocol specifies a <findService> request. The ECRF responds to <findService> requests as well as other LoST protocol requests. GeoComm ECRF is provisioned with the aggregated GIS dataset supplied by the State. Authorized i3 functional elements, such as an NG9-1-1 ESRP, may query the GeoComm ECRF with a geodetic or civic location and a service URN describing the type of service requested, in a LoST <findService> request. ECRF queries the GIS database that has been provisioned to it in order to discover and return a service URI, which is used by the ESRP to send the call to the correct next hop destination.

7. Provide a clear description of the functionality of the ECRF; list features and capabilities.

GeoComm ECRF and LVF

GeoComm ECRF and LVF are IETF RFC 5222 compliant servers which provide the NENA i3 functional elements of ECRF and LVF specified in NENA-STA-010.2, the second version of the i3 Standard (originally NENA 08-003). In addition to these standards, there are many related RFCs that define how the ECRF and LVF operate, including PIDF-LO, RFC 4119, and its revision RFC 5139.

GeoComm ECRF and LVF utilize a load balanced, multi-server architecture supporting geographic redundancy with no single point of failure, and physical separation between ECRF and LVF systems and databases. GeoComm ECRF and LVF:

- Provide fast, secure, and reliable core network ECRF services for NG 9-1-1
- Enable fast geo-spatial 9-1-1 call routing and location based selective transfers
- Provide industry standard i3 location validation
- Include and ad-hoc routing boundary editor
- Include a Network Operations Center (NOC) dashboard, and monitoring and reporting capabilities
- Were tested for interoperability at NENA ICE 1-8, and EENA/ETSI Plugtest #1
- Support NG 9-1-1 additional data discovery
- Accept NENA i3 standardized Spatial Interface (SI feeds) for ingesting GIS updates
- Accept proprietary GIS data updates from non-NENA standard systems
- Contain a dashboard suitable for display in a NOC
- Support NENA i3 logging, Simple Network Management Protocol (SNMP), as well as raw log data outputs for third party monitoring and logging solutions.
- Integrate seamlessly with the proposed GIS Data Hub system

ECRF and LVF Features

GeoComm ECRF is an IETF 5222 compliant LoST server system, providing the NENA i3 ECRF functional element as defined in NENA-STA-010.2. General features of the GeoComm ECRF include:

- IETF RFC 5222 compliant LoST Server
- NENA-STA-010.2 compliant ECRF
- Calculates service URI for 9-1-1 call routing and selective transfer based on a call's location
- Can play multiple roles in LoST hierarchies, including Forest Guides, state level ECRFs, and regional "leaf node" ECRFs
- Administrative dashboard for monitoring real-time statistics, load, query response behavior, and individual query contents, system-wide and per server

- Supports NENA i3 logging mechanisms, includes internal logging, and provides network monitoring system interfaces
- Architected to support a fully redundant, secure, multi-tier load balanced server architecture
- Supports PIDF-LO geodetic location types of point, polygon, circle, ellipse, and arc-band
- Supports PIDF-LO civic location types, including fine grained components handling building, floor, suite, room, and seat
- Facilitates the discovery of additional location data, by complying with the additional data discovery mechanisms described in NENA-STA-010.2. GeoComm ECRF supports discovering additional data using all location types defined in RFC 5222 – civic locations (including optional sub-address elements), points, circles, polygons, ellipses, and ArcBands.
- Supports the discovery of agency locator records as defined in NENA-STA-010.2
- Supports multiple provisioning interfaces:
    - A NENA i3 standards-compliant SI for provisioning change-only GIS data updates in near real time, on a scheduled or ad-hoc basis
    - Custom ETL: suitable for interoperating with other proprietary GIS enterprises
    - Bulk update capability for use during initial system provisioning, mass GIS data updates, or in less frequent instances, system upgrades and fault recovery

GeoComm ECRF Advanced Features

GeoComm ECRF also includes many advanced features not commonly available in other vendor ECRF implementations. GeoComm ECRF provides secure web-based administration, including on-the-fly, ad-hoc routing boundary changes. Ad-hoc routing boundaries are useful to implement geographic-based routing changes during wide-scale emergency events when call routing needs to be changed quickly. During such events, it may not be practical to request a service boundary change to be implemented by the GIS data management staff and propagated to ECRFs via the agreed upon ECRF GIS data provisioning mechanism.

GeoComm ECRF ad-hoc routing boundary feature makes it possible to draw a new temporary routing boundary around an area and designate a PSAP service URI for the temporary polygon. From that point forward, instantly, all 9-1-1 calls originating within that area will route based on the new temporary service URI, which could point to a different PSAP, or a virtual PSAP deployed in the field. As a policy decision, Nebraska may decide to allow or disallow the use of ad-hoc routing boundaries in ECRF.

GeoComm ECRF supports additional service types beyond "9-1-1 PSAP" which is commonly used when routing a 9-1-1 call to a PSAP. After a 9-1-1 call has been answered, an authorized NG 9-1-1 PSAP CTI application may query the ECRF with the location of a 9-1-1 caller, and a service uniform resource name (URN) indicating a type of service desired for call transfer, such as particular responder agency. In this manner, GeoComm ECRF supports geospatial selective 9-1-1 call transfers, which can reduce the time it takes to transfer a 9-1-1 call and decrease chances of transferring a 9-1-1 call to the correct agency.

GeoComm ECRF includes the ability to discover additional data associated with a location. NENA 71-001 NG 9-1-1 Additional Data describes several additional data information data structures, such as additional data associated with a call, associated with a caller, and associated with a location. The additional location information data structure is discovered by querying an ECRF additional location data service. GeoComm ECRF fully supports the additional data discovery mechanisms defined in NENA-STA-010.2.

This enables <findService> requests for additional data when using the special service URN urn:nena:service:additionalData. When queried in this manner, GeoComm ECRF will search for address points that have a URI to additional data associated with a location document which can describe a myriad of information (see NENA 71-001 – NENA Standard for NG9-1-1 Additional Data).

8. Describe the error handling, default mechanisms, and logging; and

Default Mechanisms

GeoComm ECRF can return a default route URI for requests containing locations that did not properly resolve within the loaded GIS coverage area. This can happen when a location is slightly incorrect, such as an invalid house number. It can also occur when new addresses have not yet been loaded into the ECRF.

GeoComm ECRF also implements a “best efforts” scheme in the event a civic location provided in a LoST <findService> request does not completely match GIS data that has been provisioned to the ECRF. In the example provided in the requirement of a civic location containing an unrecognized street name, but valid city and state, GeoComm ECRF can return a service URI based on a PSAP service area boundary polygon wholly containing the civic location’s city. In this case, the <findServiceResponse> returned from GeoComm ECRF will also contain a <defaultMappingReturned> warning,

indicating to the querying function that a default mapping was then determining the route. This "best efforts" feature in the ECRF is a configurable option that may be turned on or off as a matter of policy.

Error Handling and Logging

GeoComm ECRF can capture unhandled exceptions and still return a response to the requestor indicating an internal error occurred. In addition, several other potential error conditions are checked for and reported back to the requestor including:

- Malformed XML or LoST syntax (bad request errors)
- Requested service URN is not supported (service not implemented errors)
- Invalid GML or coordinate values (location invalid errors)
- Unknown location profiles (location profile unrecognized errors)
- Spatial reference problems (SRS invalid errors)
- Revisiting an already queried server (loop errors)
- Recursive time out conditions (server timeout errors)
- Bad response from a recursively queried server (server errors)
- Access denied to recursively queried server (forbidden errors)

GeoComm ECRF has several logging mechanisms to facilitate transaction auditing, debugging, and activity monitoring. Diagnostic logs exist for all servers in the system, tracking any internal server errors that occur, which can then be analyzed for configuration and server errors. In addition, all LoST transactions are logged for a complete archive of activity. Logging mechanisms also include i3-compliant log event reporting. This means that, within an ESInet, the servers can send ECRF request/response logs to an i3 compliant logging service. Finally, the ECRF includes a browser-based dashboard which shows current activity and server status, generates transaction reports, and views the logs directly.

9. Provide an overview of deployment recommendations to achieve 99.999 percent reliability.

High Availability Deployment Architecture

The GeoComm ECRF architecture is a load balanced, fault tolerant system of GIS servers, database servers, and web servers deployed using docker containers and Kubernetes, with no single point of failure, and is capable of 99.999% uptime when deployed across multiple data centers. To meet the 99.999% up time requirement the system is designed with N+1 capacity and redundancy on all tiers.

Each data center contains multiple redundant GeoComm ECRF containers. In the unlikely event of system failure, three of the six physical machines in the ECRF system could fail and the system would still have the capacity to support the entire State. Geographic load balancing across the four ECRF servers in the two data centers increases the system's ability to spread load during peak capacity events, maintaining very low response times, and to facilitate server maintenance and updating without taking the overall system offline. GeoComm ECRF/LVF is also fault tolerant with respect to hardware; the system detects server failures and automatically directs traffic to healthy servers. The design specified is based on a 50K request per hour design with additional scaling available.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 51.				

Any additional documentation can be inserted here:

Over time, as the State interconnects its ESInet with other ESInets at a state or regional level, a degree of coordination and interaction between ECRFs and LVFs are required. GeoComm ECRF, as proposed, will reside within the State's ESInet, and will be authoritative for routing calls which ingress the State ESInet. Other ESInets will maintain their own authoritative ECRFs, responsible for routing calls within their networks. These ECRFs can be related to one another and organized into a hierarchy to form trees, as detailed in Request for Comments (RFC) 5582 and NENA STA-010.2 section 5.14. It is the interconnection of

ESInets and the relationship of ECRFs to one another which allow NG 9-1-1, via its i3 architecture, to seamlessly route and transfer emergency calls between ESInets using spatial routing technology.

The fact that networks are interconnected and ECRFs can route calls spatially provides opportunities to add fault tolerance and service continuity options throughout the ESInet hierarchy. The GIS data provisioned to an authoritative ECRF can be shared with other ECRFs, allowing those ECRFs to take over service for an authoritative ECRF if it enters a failed or inoperable state. While under normal operation, only one ECRF can be authoritative for a given geography and service uniform resource name (URN). However, in situations of irregular operations such as overload or failure, the failed or degraded ECRF could be relieved of its responsibility by its parent ECRF or one of its sibling ECRFs. The operator of another ECRF could adjust its coverage region so it becomes temporarily authoritative for the geographic region and service URNs supported by the original ECRF. So long as the other ECRF has the same GIS data as the failed ECRF, and its coverage region is modified to reflect the change in authority, the other ECRF can take over the failed ECRF's duties. To help facilitate such an arrangement between the State and its parent/sibling ECRFs, GeoComm could provision a replica of the State's GIS data to the parent/sibling ECRFs, using the GeoComm Spatial Interface, to ensure the ECRFs have the GIS data they need to take over in a moment of crisis or need. As a manner of course, the other ECRFs may employ various proprietary processes to physically "swap" or take the role of the State ECRF, as no two ECRFs can claim – at the same time – that they are both authorities for the same geographic region and service URNs.

Access/origination networks (OSPs) have a role to play in the ESInet and ECRF hierarchy as well. An OSP may elect to operate a non-authoritative ECRF replica to direct calls to the State ESInet ingress, using the same GIS data as the State ECRF or a subset of it (such as administrative and service boundaries, as in some cases, an ECRF equivalent may not need road centerlines and site/structure address points to determine the ESInets responsible for handling calls). This would require the origination service providers to separately purchase an ECRF and implement it within their networks, at which point GeoComm may assist the State in provisioning a replica of the State's ECRF's GIS data (or a subset) to the ECRF(s) operated by the OSP(s), upon request.

When provisioning GIS data to other authoritative ECRFs at the state or regional level, or to non-authoritative ECRFs operated by OSPs, GeoComm will leverage the Spatial Interface to provision data in serial fashion, one ECRF at a time. While the State ECRF could itself leverage a spatial interface to "push" its data to one or more subscribing ECRFs, GeoComm does not recommend this approach as it places an unnecessary burden on the State ECRF: once data is provisioned to it, it must then in turn replicate it to other consuming ECRFs, and leveraging a single Spatial Interface to replicate data in serial fashion provides a single place to monitor and manage the data replication activity to all ECRFs.

In the context of this requirement, GeoComm understands "replica" is speaking to data replication and nothing else.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 52.				

Any additional documentation can be inserted here:

Only one ECRF is authoritative for a geographically defined region. Data can easily be aggregated using the hosted spatial interface (SI) for higher level non-authoritative ECRFs and GeoComm also supports LoST sync from the ECRF to provide data to the forest guides.

Using higher level routing functions is at the discretion of the OSP. GeoComm has experience supporting multiple different deployment types.

As described in the previous response, ECRFs are organized into hierarchies and trees. Because one and only one ECRF/LVF can be authoritative for a given region and service URN, there must be a means to easily discover which ECRF is responsible for answering a query. As it is unlikely in the long term that each ECRF within a tree will contain the coverage regions of all

other ECRFs, it is recommended that Forest Guides be employed to help an ECRF client discover the appropriate authoritative ECRF to answer their queries. Forest Guides can, and should, always be present, to help guide requests to the proper authoritative ECRF/LVF for the given geography and service URN. While GeoComm recognizes there are no operational Forest Guides in existence today, and that interconnection between ECRFs can be achieved by sharing ECRF coverage regions amongst ECRFs in a hierarchy and within the trees, Forest Guides are critical to the success of spatially routing emergency calls using ECRFs in the i3 end state.

		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: Hamilton complies with requirement NGCS 53.				

Any additional documentation can be inserted here:

GeoComm LVF is an IETF 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF/LVF as specified in NENA TSD 08-003. GeoComm LVF is includes the following features:

- IETF 5222 compliant LoST Server providing NENA i3 LVF
- Validates civic locations prior to entry into a LIS using the LVF
- Can play multiple roles in LoST hierarchies, including Forest Guides, state level LVFs, and "leaf node" LVFs
- Supports PIDF-LO geodetic location types of point, polygon, circle, ellipse, and arc-band
- Supports PIDF-LO civic location types, including fine grained components handling building, floor, suite, room, and seat

GeoComm LVF is designed in accordance with the NENA standards. The LVF will be authoritative based on the GIS data provisioned into the system.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 54	**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**.**	X			
	Bidder Response: Hamilton complies with requirement NGCS 54.				

Any additional documentation can be inserted here:

GeoComm GIS Data Hub serves as the user interface to supply the GIS data to the system and manage the Spatial Interface. After the data has passed required QC checks, the GIS data is transferred to the NENA required schema then added to the spatial interface. GeoComm ECRF and LVF consume XML GIS changes and confirm changes once applied to the production dataset. Updating the production GIS data does not impact ECRF or LVF availability.

GeoComm also provides a bulk load feed to ensure ECRF and LVF have access to the full GIS dataset. This ensures that if a data synchronization issue is detected, the whole GIS dataset can be loaded without system disruption or for use in fault recovery scenarios.

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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 55.				

Any additional documentation can be inserted here:

The LVF will be available as an external function for validation of civic addresses.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 56.				

Any additional documentation can be inserted here:

The GeoComm LVF architecture is a load balanced, fault tolerant system of GIS servers, database servers, and web servers deployed using docker containers and Kubernetes, with no single point of failure, and is capable of 99.999% uptime when deployed across multiple data centers. To meet the 99.999% up time requirement the system is designed with N+1 redundancy on all tiers.

NGCS 57	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 57.				

Any additional documentation can be inserted here:

An LVF is inherently public facing and external to the ESInet. Service providers may query GeoComm LVF. Due to the nature of the network connections, the service providers will query LVF “publicly.”

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 58.				

Any additional documentation can be inserted here:

NENA Compliance

GeoComm LVF is an IETF 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF/LVF as specified in NENA-STA-010.2-2016.

Availability

To ensure the LVF proposed remains highly available, GeoComm LVF will be deployed in a fully redundant clusters load balanced across two data centers. The GeoComm LVF system will be provisioned using the same mechanisms and data as GeoComm ECRF which will ensure the system is kept as available and current as possible. As designed, the LVF system is easily expandable, allowing for additional redundancy and capacity as the region requires, by implementing additional hardware to the system.

Supported Interfaces

GeoComm LVF supports the LoST interface. The external ECRF supports the LoST interface.
The proposed system can be expanded to support the MCS interface and geocode interfaces.

User Interface

GeoComm LVF is equipped with an operations portal for monitoring real-time statistics, load, query response behavior, ad hoc routing and individual query contents, system wide and per server.

Documentation

GeoComm LVF can be utilized directly by any authorized 9-1-1 entity needing to perform NG9-1-1 i3 location validation in place of or alongside legacy 9-1-1 MSAG style validation. GeoComm LVF uses site and/or structure layers and address ranged road centerline layers.

In i3 networks, MSAG is replaced with a GIS based LVF. Before civic address locations are entered or updated in a Location Information Service (LIS), the address records must be validated to ensure they are adequate for routing, dispatch. This is accomplished by locating the civic address in the authoritative GIS database for the service area:

LVF queries include a validateLocation=true attribute. When this attribute is present and set true in the query, GeoComm LVF treats the request as a location validation request, and returns a LoST <findServiceResponse> which includes location validation elements stating which parts of the provided civic location passed validation, failed validation, or were unchecked.

Features

- IETF 5222 compliant LoST Server providing NENA i3 LVF
- Validates civic locations prior to entry into a LIS using the LVF
- Can play multiple roles in LoST hierarchies, including Forest Guides, state level LVFs, and “leaf node” LVFs
- Supports PIDF-LO geodetic location types of point, polygon, circle, ellipse, and arc-band
- Supports PIDF-LO civic location types, including fine grained components handling building, floor, suite, room, and seat

Security

GeoComm LVF is publicly available web service using https and TLS. Access will be controlled by Hamilton's security procedures.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 59.				

Any additional documentation can be inserted here:

GeoComm SI is a NENA compliant spatial interface that allows any subscribed application to get changes to the statewide GIS dataset, including applications that consume an SI such as the PSAP tactical map display, CAD systems, and similar applications. The system provides a means to ingest, analyze, and report on, GIS data from the State's authoritative GIS dataset, suitable for provisioning to GeoComm ECRF or LVF and other Functional Elements.

In addition, as a NENA i3 compliant SI, GeoComm SI transmits GIS data updates from the authoritative GIS database system and applies them to ECRF and LVF databases.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 60.				

Any additional documentation can be inserted here:

GeoComm will work with the state of Nebraska to establish a mutually agreeable daily schedule for GIS data provisioning, including a daily deadline to submit GIS changes for processing. The State could expect data submitted prior to the daily deadline to undergo QC checks and, within 24 hours of the data passing required QC checks, it would undergo a series of transformation measures to convert the data into the format required by the ECRF and LVF. Then, it would be transferred from GeoComm SI to the ECRF and LVF. GeoComm SI uses a NENA i3 compliant SI provisioning feed to accomplish the transfer.

Data not passing validation checks would be returned to the State for error resolution. After data errors have been resolved, the State would then resubmit the statewide dataset back into the system for processing, following the same mutually agreeable submission deadline. This ensures the data provisioned to ECRF and LVF is always the most current and accurate data available. Data submitted after the daily deadline would be processed after the following day's deadline.

While the state confirmed its responsibility at this time for the quality of the data incorporated into the authoritative dataset, GeoComm will provide the ongoing QA/QC audits. GIS data remediation services are available upon request and GeoComm would work collaboratively with the state to negotiate this additional service if desired.

As an option, for an additional fee, GeoComm could provide customized GIS extracts of public safety grade GIS data to be ingested into CAD maps or other applications which consume GIS data. The extracts would be provided to the State/local data authorities who would be responsible for provisioning to the associated application.

NGCS 61	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 61.				

Any additional documentation can be inserted here:

GIS data updates from the authoritative GIS database are transmitted and provisioned to the ECRF and LVF via the SI. Assuming updates are being made to the GeoComm ECRF and LVF, the NENA i3 compliant Spatial Interface provisions change-only or bulk GIS updates in near real time on a scheduled or ad-hoc basis. However, should a different ECRF or LVF be deployed, the proposed SI is compatible with any ECRF or LVF meeting industry standards. In this scenario, the data provisioning methodology may vary from that which would be executed with GeoComm ECRF and LVF.

Before GIS data can be used for routing 9-1-1 calls and validating civic locations in an NG9-1-1 system, the accuracy and integrity of the data must be validated through a series of data-specific QC procedures. GeoComm will work with project stakeholders to develop a formal QC plan. The quality control approach, including regular communication of QC results to the State, will be documented in the plan.

Upon data upload, GeoComm SI scans the submitted data files to ensure they are not corrupted and processes the data through a change detection process to identify features differing from the previous GIS datasets uploaded. These changes are then validated by the system to ensure they can be applied to the master GIS database without negatively impacting 9-1-1 system operation. If no validation failures are detected in the submitted data, the changes are applied to the master GIS dataset.

Once the system is cut over, data passing QC checks in the system will continue processing without interruption. Data will be provisioned within 24 hours after being processed through the QC checks. Datasets not passing validation checks will be returned to the submitting agency for error resolution.

As mentioned above in NGCS 60, while the state has confirmed its responsibility at this time for the quality of the data incorporated into the authoritative dataset, GeoComm will provide the ongoing QA/QC audits. GIS data remediation services are available upon request and GeoComm would work collaboratively with the state to negotiate this additional service if desired.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 62.				

Any additional documentation can be inserted here:

GIS Data Hub is a user-friendly web-based GIS management system that allows secured access to upload GIS layers for use in the next generation 9-1-1 system. GIS Data Hub will provide ongoing GIS data transformation, QC, and reporting which will result in the progressive improvement of the State's NG 9-1-1 GIS dataset. GIS Data Hub provides e-mail notifications as data is processing through the system, with granularity that can be configured for each type of GIS data manager. Based on each

user's notification preferences, they can receive reports that include PDF reports, GIS error layer files, csv docs of non-geospatial errors, ETL fallout, and processing times. Data subscribers can be notified when new data has passed QC checks and is ready for download.

The State would upload GIS updates to GIS Data Hub on an up-to-daily basis using a zip file, to be processed through multiple QC checks. The default QC checks within the system are based on the NENA data model and additional QC checks will be configured to reflect State of Nebraska data standards. The QC checks would be executed prior to any data updates being incorporated into the statewide GIS dataset to ensure only accurate GIS data is included in the NG9-1-1 GIS dataset used in the ECRF and LVF.

After the data has been processed through the QC checks, a digital data quality report will be delivered back to the State. Data passing the QC checks will be transformed into the format required for NG9-1-1 operations to ensure the dataset is compliant with NENA and State standards.

Source data not passing the initial QC checks will be referred back to the State for data error resolution, with errors outlined in the digital data quality report delivered by the system. The State will be responsible for correcting the data errors and resubmitting the updated data to the system.

This process would be followed for both initial and ongoing GIS updates, resulting in a continuous feedback loop of GIS data updates from the State, GIS data performance measurements and reporting, and data transformation.

Because GIS Data Hub accepts GIS data in its native format, it can accommodate difference schemas should different authoritative sources have varying data schemas. There is no need for the State to change its original GIS data model schema; GIS Data Hub automatically modifies the input data schema to adhere to the required output. This means the process of incorporating data updates and changes will have minimal impact on existing data management operations.

Monitoring

GeoComm manages the system and data flow through the GIS platform on behalf of the State. System users will be granted varying levels of access to data and QA/QC reports within the system. This will result in a hierarchy of users which are defined by the State. GIS Data Hub hardware and security will be monitored by the overall solution monitoring methodology.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 63.				

Any additional documentation can be inserted here:

The LDB can interface with any neighboring ESInets, but it is likely to need to interface directly with other LDB solutions. If a call originates in Nebraska, and is transferred over a state line to another NENA i3 compliant ESInet, the location dereference URL will go with the transfer in the SIP header. The CHE across the state line can use this dereference URL to obtain the callers location directly from the NE LDB, without the need to utilize any LDB within their own state.

As an example, a wireless call placed from South Dakota may hit a cell tower in Nebraska. This call will likely hit an LNG in Nebraska, which will in turn query the Nebraska LDB. Once at the Nebraska ESRP, one of two things can happen. The ESRP will dereference the location from the Nebraska LDB. If the LDB is only able to return a cell tower location at this point, the call will be routed to a Nebraska PSAP. From there, the PSAP can transfer the call to the South Dakota PSAP. This transfer will include the location dereference URL that the South Dakota PSAP can use to get updated location information from the Nebraska LDB. Alternatively, if the Nebraska LDB can return the actual callers location to the Nebraska ESRP and the ESRP can route the call directly to the South Dakota ESInet (to either the South Dakota ESRP or directly to the appropriate South Dakota PSAP). If sent to the South Dakota ESRP, it can use the dereference URL to request updated location from the Nebraska LDB and use that to determine which South Dakota PSAP the call should go to (using the South Dakota ECRF).

If a neighboring state is still legacy or not fully NENA i3 complaint, other mechanisms can be put in place, such as legacy style FoCR. In this situation, pANI records in the Nebraska LDB are shared with the neighboring state for them to provision in their ALI database. Conversely, the neighboring state will share their pANI records for provisioning in the Nebraska LDB.

NGCS 64	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 64.	X			

Any additional documentation can be inserted here:

In order for an LDB to function correctly and allow interoperability between legacy and Next Generation 9-1-1 formats, a MSAG Conversion Service (MCS) is needed (as defined in NENA-STA-010.2-216). An MCS is included as part of this response.

MCS Overview

The MCS is designed to bridge the gap between legacy (ALI/MSAG) and Next Generation (PIDF-LO/CLDXF) data schemas and formats. An MCS is a required functional element if interoperability is required between legacy and Next Generation data.

In the situation where the legacy ALI database is wholly replaced by a transitional Location Database (LDB), the MCS is used by the Service Order Input (SOI) process to convert the legacy address records submitted by the service providers to the NG 9-1-1 CLDXF format. The LDB stores all records in CLDXF format and is therefore closely aligned with the data in the ECRF/LVF. Additionally, the MCS is used to convert dynamically received address data that is received over an E2 connection (typically for VoIP). E2 will return address data in a legacy format, which needs to be converted to a CLDXF compliant PIDF-LO before being sent to the ECRF for call routing instructions.

If legacy CHE exists in the deployment, the MCS will also be used to provide legacy ALI services to this CHE.

Without the MCS, location data associated with each call will not be aligned with the GIS data that is in the ECRF/LVF, as this data is required to be in the NG 9-1-1 GIS Data Model (which is closely aligned with CLDXF, and very different from legacy ALI/MSAG data models). Failure to align call location data with ECRF/LVF data will result in significant call routing issues.

Additionally, the MCS can provide translation services to gateway elements when calls need to be transferred with location between legacy and NG PSAP's.

LDB Overview

To overcome the problems of legacy ALI systems, NENA recommends the use of the Location Interwork Function, or LIF, within the Legacy Network Gateway, utilizing an internal location database with steering data as needed. This database is often referred to as an LDB, or Location Database (NENA-INF-008.2-2014). The LIF is a part of the LNG, although it can be physically separated.

A Location Database (LDB) serves as both a legacy ALI database and as a LIS in an i3 NG 9-1-1 environment and is included in this response to fully replace the existing ALI database and enable smooth transition to NG 9-1-1.

The LDB can provide the same functionality as a legacy ALI database, but also provides i3 processes and interfaces. A single state-wide LDB would provide numerous advantages over the current ALI database system(s), including:

- All location records that contain a civic address are pre-validated against the LVF, ensuring that at the time of a 9-1-1 call they will properly route. LDB response times are measured in milliseconds, not seconds (note that for wireless and nomadic VoIP, the LDB must still communicate with MPC/VPC which will introduce delay).
- Service providers would not have to change their workflows, as the LDB supports the legacy SOI provisioning interfaces. Service providers can continue to send their records in this legacy format, and the MCS will be used to convert the record into the NG 9-1-1 data model before provisioning the data into the LDB. This means that legacy service providers can continue "business as usual", without having to change their existing processes.
- All data would be stored in native NG 9-1-1 formats.

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).

NENA 02-010 Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping

The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-010. The LDB supports Service Order Input (SOI) processing of files in the 2.1 and 4.0 exchange formats. Support for version 3.0 is not implemented as it is not commonly used within the industry. The GIS data model is not directly relevant to the LDB.

NENA 02-011 NENA Data Standards for Local Exchange Carriers, ALI Service providers & 9-1-1 Jurisdictions

The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-011.

NENA 02-015 Standard for Reporting and Resolving ANI/ALI Discrepancies and No Records Found for Wireline, Wireless and VoIP Technologies

The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-015. All "No Record Found" reports are automatically generated for service providers, and the LDB Manager web interface provides a full NRF workflow. Location discrepancies (such as those reported by a PSAP) are tracked in the standard ticketing system.

NENA 04-005 NENA ALI Query Service Standard

The LDB stores location data in a format compliant to the NG 9-1-1 data models. This means an intermediate process is required to convert this data for legacy ALI. If an AQS is required, an MSAG Conversion Service (MCS) is used to convert the CLDXF compliant PIDF-LO from the LDB back into the NENA ALI 4.0 format. At this time the AQS is not fully supported, but can be if required.

It is recommended that CPE use the NG 9-1-1 HELD protocol wherever possible. Legacy ALI interfaces do not support the same rich data format as HELD. If all CPE can support the HELD protocol, there is no need for an AQS to be deployed. Standard legacy ALI is fully supported.

NENA 08-501 NENA Technical Information Document on the Network Interface to IP Capable PSAP

The entire LDB is built to communicate over IP networks, and fully supports both IPv4 and IPv6. Legacy ALI queries can be supported over a TCP/IP connection, and the HELD interface also runs over a TCP/IP connection.

The LDB also supports additional data when using the HELD protocol. The latest standards are used for this, which supersede the information in this document.

NENA 08-502 NENA Generic E9-1-1 Requirements Technical Information Document

The LDB supports section 2.6.2, with the exception that the location information is LVF validated rather than MSAG validated.

The LDB provides callback information as described in section 2.6.3, providing the callback information is available from the MPC/VPC.

The LDB supports section 2.7.2 in that it will store static location data, as well as steer E2+ queries as appropriate for nomadic location data, such as wireless and nomadic VoIP.

The LDB can process SOI files from Service providers in either the NENA 2.1 or NENA 4.0 formats, as described in section 2.7.2.1. A full range of error and validation checks are performed on each file and each record and errors are returned to the Service provider for resolution. LVF generated discrepancies are returned to the GIS group responsible for the data in the ECRF/LVF.

Local number portability (LNP) is fully supported through the use of the Unlock and Migrate process, and NPAC databases are queried to verify TN ownership to ensure the accuracy of the database.

The LDB supports section 2.7.2.2, offering both legacy and i3 interfaces for location queries. NG 9-1-1 compliant CPE can use the HELD interface, whereas legacy systems can perform a legacy ALI dip.

The ability to steer queries to other databases is supported, as described in section 2.7.2.3, but requires full cooperation of other database providers.

The LDB includes a full ESME subsystem, allowing it to communicate over E2/E2+ to positioning centers for wireless and nomadic VoIP.

The LDB can be deployed in a multiple node system, allowing it to achieve 99.999% availability as described in section 2.7.2.5.

The LDB meets the requirements of section 2.7.2.6, as most queries for static records take 100 ms or less. Queries to outside systems (such as an MPC/VPC) may take longer and are beyond the control of the LDB.

The LDB supports data provisioning as described in sections 2.8.2.1 and 2.8.2.2, using either standard SOI type file processing or a web interface.

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.

The LDB was developed to provide all the relevant transitional database functionality as defined in section 11.5 of the NG 9-1-1 Transition Plan Considerations document. Unlike other solutions on the market, our LDB was built from the ground up as an LDB, not an ALI database system repurposed as an LDB.

Shall support NENA standards J-036, E2, E2+, non-call-associated signaling (NCAS) and call-associated signaling (CAS).

The LDB, in conjunction with the ESME, can provide all the necessary processing to handle legacy wireless and nomadic VoIP calls.

In a typical scenario, each pANI record within the LDB is assigned to an E2 connection (E2 steering). The ESME sub system maintains all E2 connections to the appropriate MPC or VPC. When a pANI query is presented to the LDB, it determines which E2 connection it needs to use, and passes a query onto the ESME. The ESME, which has dual IP connections to each MCP or VPC, performs the actual E2 (or E2+) query to the appropriate positioning center, and passes the response back to the LDB.

In the case where the E2+ response contains a address (often occurs with nomadic VoIP), a further call in placed to the MCS to convert this address from a legacy format to the PIDF-LO equivalent.

Shall be able to provide LIS functionality and interfaces as defined in NENA-STA-010.2-2016.

The LDB supports all LIS functionality and interfaces as defined in NENA-STA-010.2-2016. Specifically, the LDB supports the HELD protocol, as specified in NENA-STA-010.2-2016, and detailed in RFC 5985, and HELD location dereference RFC 6753.

Shall be able to seamlessly interact with a NENA i3-compliant ECRF, as described in NENA-STA-010.2-2016.

The LDB, as part of data provisioning, uses the LoST protocol to validate all civic address data against the ECRF/LVF. All civic address locations that return invalid elements will generate a discrepancy and will enter into the LDB discrepancy workflow system.

In terms of call flow, the LDB and ECRF act independently. The ESRP will issue a dereference HELD query to the LDB and await a response. Once the response is received, the location will be sent by the ESRP as a LoST query to the ECRF.

Shall be able to dereference a location by reference, as defined in NENA-STA-010.2-2016.

The LDB supports both GET and POST location dereference queries using the HELD protocol.

The initial query will need to take place by value, with the initial response including the location dereference URL. Future location requests can use the location dereference URL to retrieve updated location information.

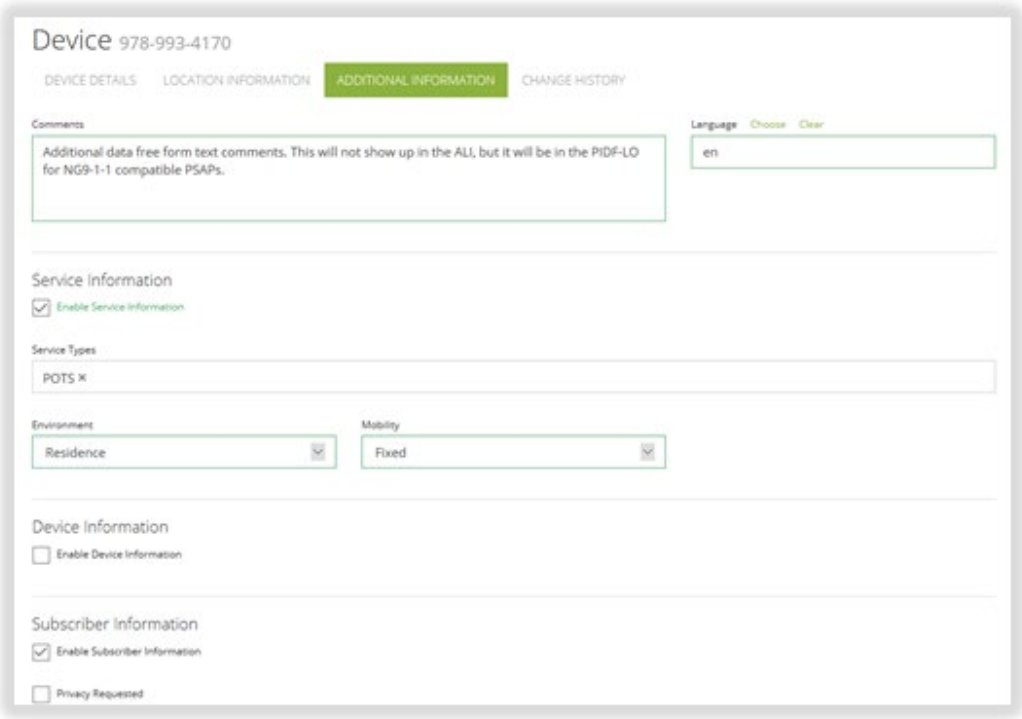
Shall be able to dereference requests for additional information, as defined in NENA-STA-010.2-2016.

Both location by value and location by reference queries include additional data in the response. The LDB currently supports the ECRIT additional data standard (RFC 7852), which includes most of the additional data structure defined in NENA-STA-010.2-2016 (such as ProviderInfo and ServiceInfo).

The following screenshot shows the LDB Manager web interface for a Device Additional Data.
that the Service Providers do not have to change current processes in order to support the i3 system (an MSAG Conversion Service is provided to convert SOI records into the appropriate CLDXF format for comparison against the LVF).

Service providers can submit their SOI files for processing via some agreed upon, secure method. Asynchronous back end server processes run to process the SOI files. Multiple SOI processing agents can be configured on a single database, allowing multiple SOI files to be processed at the same time.

Unlike SOI processing for E9-1-1 ALI databases, each SOI record must be validated against the GIS, by way of an LVF, prior to the record being committed to the database and being made available for HELD queries. This ensures the civic address location provided by the Service Provider can be mapped, and thus routed and plotted. If a record fails validation, the Service Provider is notified (various notification mechanisms exist, including an error report). The group responsible for the GIS map data can also be notified, so the map data can be checked for accuracy. The following screenshot shows the details of a SOI Job.



Shall be able to interface simultaneously with multiple wireless callers.

The LDB supports legacy wireless location delivery using an Emergency Services Message Engine (ESME) connected to one or more Mobile Positioning Centers. Each multi-threaded ESME instance can handle multiple simultaneous queries, with the ability to handle hundreds of wireless calls per second.

Shall be able to interface simultaneously with multiple remote ALI databases.

Providing that the remote ALI database provider can provide steering data (in some agreed upon mechanism, such as FoCR), the LDB is able to steer queries to remote ALI databases.

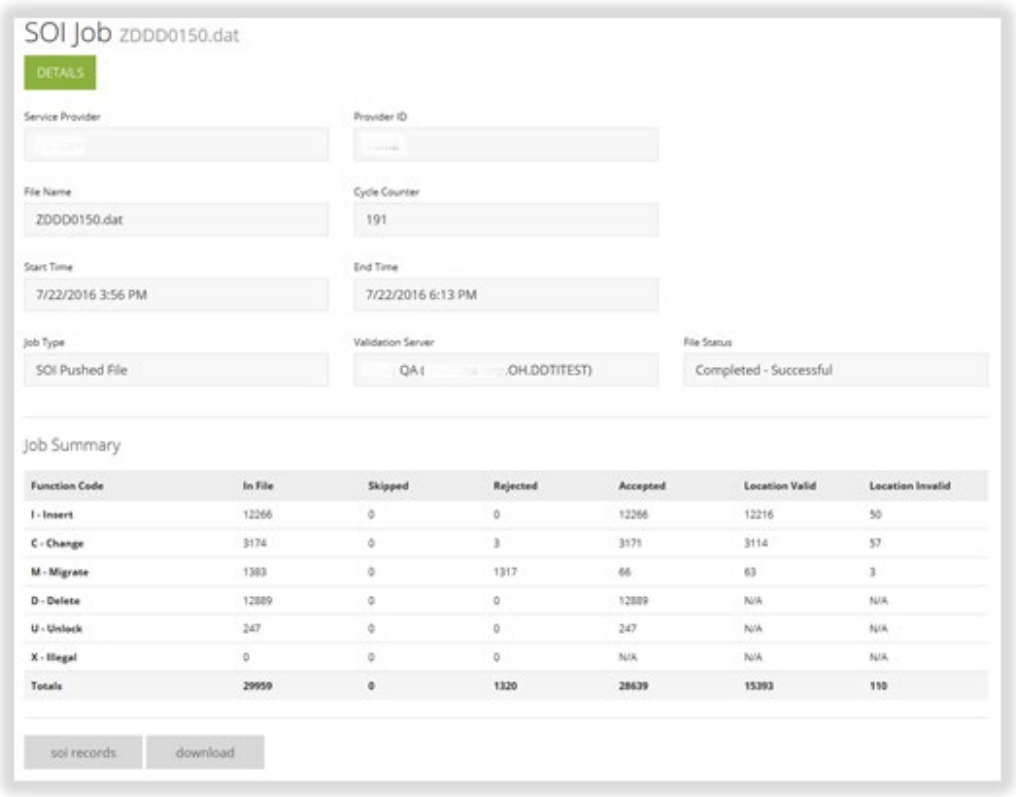
The MSAG Conversion Service (MCS) is used to convert legacy ALI response from the remote ALI database into PIDF-LO.

Additionally, the LDB can be provisioned with pANI from neighboring ALI databases, allowing it to perform E2 queries to retrieve location information for calls that have been transferred into Nebraska. Data sharing agreements must be in place with neighboring ALI database providers for the sharing of these records.

A legacy ALI interface can also be provided, allowing the legacy ALI database to perform queries for data contained within the LDB. The MCS will be used to convert the LDB PIDF-LO data into the legacy ALI 4.0 format, which can then be formatted into other legacy ALI formats.

Shall automatically detect, import and validate customer records (SOI records).

To successfully replace a legacy ALI system with an LDB, a mechanism must be provided to the Service Providers to update the location information in the LDB. During the transition to i3, and to aid 9-1-1 authorities gaining cooperation from the Service Providers, the LDB system includes a Service Order Input (SOI) processing function that is similar to existing SOI processing.



Function Code	In File	Skipped	Rejected	Accepted	Location Valid	Location Invalid
I - Insert	12266	0	0	12266	12216	50
C - Change	3174	0	3	3171	3114	57
M - Migrate	1383	0	1317	66	63	3
D - Delete	12889	0	0	12889	N/A	N/A
U - Unlock	247	0	0	247	N/A	N/A
X - Illegal	0	0	0	N/A	N/A	N/A
Totals	29959	0	1320	28639	15393	110

This means each SOI record can be looked at individually also. Records that are rejected can be directly edited within the LDB Manager web interface, or a new and correct SOI record could be submitted.

Scheduled, periodic revalidation of existing LDB records will also be performed by the system. This process checks all LDB records that have previously been flagged as LVF valid and submits a new LVF query to verify each record is still valid. Records that fail validation will be flagged in the LDB as invalid but will still be returned in HELD queries for a configurable time period (by default, this is 30 days), allowing the Service Provider or GIS department time to investigate and resolve the issue.

The LDB utilizes a web-based interface allowing authorized personnel access to the backend location database. From this web interface, users with the appropriate permissions can schedule reports and data extracts to be run.

Key functionality of the web interface includes:

- Role based security, restricting users to what they can do and what data they can see. For example, a Service Provider will only be allowed to view their location records and job reports from SOI jobs they have submitted.
- Ability to query data by telephone number and address.
- Ability to modify location records and validate the changes against the LVF in real time.
- View reports.

Workflow for resolving data discrepancies for records that have failed LVF validation (for example, if, after review, the Service Provider has determined that the location data is correct, the discrepancy can be routed to the appropriate GIS department for resolution).

Users can be defined and managed via the LDB web interface. Users will have permission-based access to their subscriber data and be able to schedule daily data extracts.

Shall have the ability to be used simultaneously by both NG911-capable and E911 capable PSAPs.

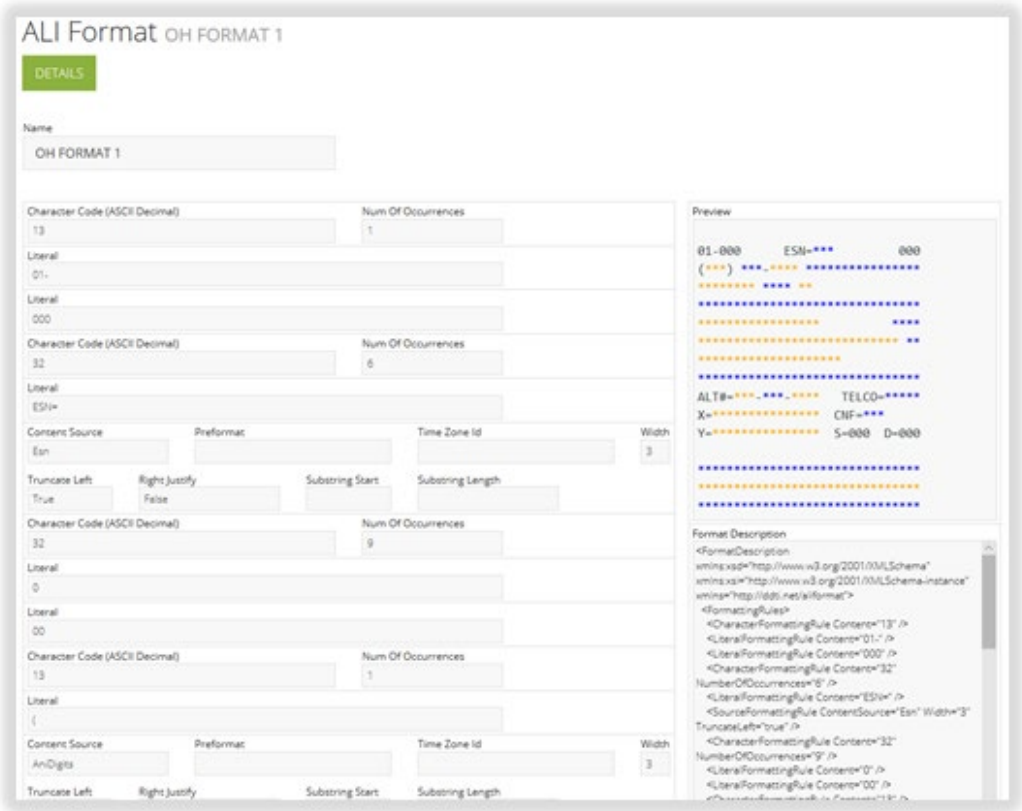
The LDB provides both legacy and NG 9-1-1 location interfaces. To support NG 9-1-1 capable PSAP's a HELD interface is provided. To support legacy PSAPs, a legacy ALI interface is provided, and location data within the LDB is converted into legacy formats using the MSAG Conversion Service.

The HELD interface can support hundreds of queries per second. The legacy ALI interface requires the legacy CPE to maintain one or more TCP/IP connections. Each CPE instance must initiate and maintain the connection to the LDB legacy ALI interface. Each individual TCP/IP connection can handle one legacy ALI query per position at a time. This is a limitation of the legacy interface, not of the LDB.

Shall allow different PSAPs to use different ALI formats based on individual needs.

It is expected that NG 9-1-1 capable PSAPs will not use ALI at all and should be capable of consuming data provided in the HELD response. Data provided in this way cannot be reformatted into different formats as it is controlled by a well-defined XML schema.

For legacy PSAPs that use the legacy ALI interface, the response can be formatted on a PSAP by PSAP basis. The following screenshot shows the ALI formatting page.



Shall utilize LVFs to validate civic addresses.

As civic address data is provisioned into the LDB (either through SOI or by manual input using the web interface), it is validated against the LVF. If the civic address is submitted via SOI, it is converted from legacy MSAG format to the LVF compatible

CLDXF format before being validated by the LVF. If a civic address fails validation, it is placed into the discrepancy workflow process for resolution.

Discrepancies are marked with a severity that is determined from the response from the LVF. A civic address that fails to return a mapping will be flagged as critical, allowing these types of discrepancies to be worked first.

Shall support PIDF-LO location data formatting as defined in NENA-STA-010.2-2016.

The CLDXF standard describes the PIDF-LO format for the United States. This standard is strictly observed in both the LDB and ECRF/LVF systems. To support legacy processes (to convert between PIDF-LO in the CLDXF format and legacy ALI) an MSAG Conversion Service (MCS) is used. The MCS is included as part of this response.

All GIS data within the ECRF/LVF will be in the CLDXF format. As a result of this, the civic address data stored within the LDB must also be in this format, otherwise it would fail LVF validation. If SOI is used to provision civic address data into the LDB, it undergoes transformation from the legacy format to CLDXF during file processing, with an end result of CLDXF compliant civic address in the LDB.

Additionally, if civic address data is provided from a MPC/VPC during call flow (such as a nomadic VoIP call), it is converted during the call flow by the LDB from the legacy format into CLDXF compliant PIDF-LO (using the MCS).

Shall periodically reevaluate the location information using LVF functions within the system.

A back-end server process runs continually against the LDB database. This back-end process is configured to periodically perform revalidation tasks. It is typically configured to revalidate open discrepancies with a frequency similar to the frequency that the GIS data is updated in the ECRF/LVF. Additionally, full database revalidation is typically configured to run weekly or monthly.

The LDB has three different mechanisms for revalidation:

- A full revalidation runs as a scheduled job to periodically revalidate every civic address record in the LDB against the GIS using an LVF query.
- A discrepancy revalidation runs more frequently and revalidates civic address records that were previously flagged as being LVF invalid.

Shall be able to communicate with NG911 functional elements using the SIP and HELD protocols.

The LDB provides full support of the HELD protocol, secured with TLS. The LDB can accept HELD queries from all authorized NG 9-1-1 core elements, as well as dereference requests from NG9-1-1 capable CPE performing a “re-bid”.

The LDB does not have a SIP interface at this time as none of the other functional elements offered in this solution are capable of requesting location using SIP SUBSCRIBE/NOTIFY. In general, the industry seems to have standardized on the HELD protocol. If clients capable of SIP SUBSCRIBE/NOTIFY for location exist, support can be added to a future release of the LDB.

Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response.

The LDB converts E2/E2+ responses to PIDF-LO. In the case of wireless E2, the Position Result, which contains latitude/longitude coordinates, as well as an uncertainty, is converted to a GML circle in the PIDF-LO response, and the E2 confidence is also included in the PIDF-LO. In the case of a E2+ response that includes a civic address (in a legacy format), the legacy address is converted into a CLDXF compliant PIDF-LO using the MSAG Conversion Service.

As the HELD protocol can support multiple locations per response, the LDB is able to provide all location data received in the E2/E2+ response. Additionally, the shell record location can also be included if appropriate.

Shall be able to dereference additional data requests.

The LDB can also act as an Additional Data Repository (ADR) as defined in NENA-STA-010.2. When responding to a location request, either by value or by reference, the LDB will include available additional data blocks inside the <provided-by> element of the PIDF-LO. The additional data blocks conform to the IETF ECRIT Additional Data Related to an Emergency Call standard, and may include:

- Data Provider Information
- Service Information
- Device Information

- Owner/Subscriber Information
- Comments

Clients can retrieve the additional data by performing a dereference query to the LDB using the URI received in the initial location response.

Shall consistently respond to all requests within 400 milliseconds (ms).

Average query latency is less than 50 ms for data stored locally within the LDB. If data has to be retrieved from other systems, response times will vary and are dependent on the remote system (such as a remote ALI database, RapidSOS or an MPC/VPC).

The HELD protocol supports a parameter in the query to tell the LDB how long the query client is willing to wait for a response. This is a useful feature, particularly for legacy wireless calls. In this scenario, the LNG may initiate a query to the LDB, with a maximum wait time of seconds. The LDB will, via the ESME, query the remote Mobile Positioning Center. After three seconds, the LDB will respond with the best data it has available. At this point, it is possible that the MPC was only able to return Phase I location data. However, by the time the call reaches the ESRP, and the ESRP performs a dereference request, the ESME may have received Phase II wireless data, and so the LDB will now respond to the ESRP with this updated information.

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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 65.				

Any additional documentation can be inserted here:

The LDB has full support for PS/ALI. Each PS/ALI customer must have its own registered NENA ID, as this is used to uniquely identify and securely partition their data within the LDB. The PS/ALI customers will be given access to the LDB Manager web interface, allowing them full read and write access to their records.

Additionally, the LDB can be configured with blocking ranges, restricting the access to a specific range of TN's for which the PS/ALI customer can create new device records.

Each PS/ALI customer can manage their records in the LDB by either a SOI process (if their MLTS system supports the generation of these files) or by direct editing using the LDB Manager web interface.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 66.				

Any additional documentation can be inserted here:

Currently, Hamilton has the capability to report some discrepancies and is continuing to develop discrepancy reporting from certain key functional elements (FE) as part of its roadmap. Discrepancy reporting is based on network data and a discrepancy is created/reported anytime a call is routed via a route that is not the first, or initial, option. Hamilton has the framework established within the 911 Logix system to allow the visualization of these routing decisions. In addition, Hamilton has the capability to deliver i3 logs to ECaTS MIS solution.

At this time, Hamilton is able to support the following discrepancies: event logging, default-routing, no record found, etc. To provide a full discrepancy function, custody and alerting must be components and Hamilton will work with the Commission to provide the functionalities necessary to fulfill the requirements of the contract. Additionally, it's important to note that NENA committees are actively discussing discrepancy reporting and how it is defined and supported. Hamilton is actively participating in and monitoring the outcome of these discussions and will apply newly developed standards as appropriate. Hamilton has responded to several RFP requirements recently that desire discrepancy reporting and we are fully confident that discrepancy reporting is not a long-term roadmap item.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 67.				

Any additional documentation can be inserted here:

All Hamilton provided functional elements provide i3 logs for consumption by other logging recorders.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 68.				

Any additional documentation can be inserted here:

Logging and reporting are critical components of the offered service. Hamilton leverages 911 Logix, a comprehensive logging and reporting tool. This tool ingests NENA i3 system logs from the functional elements as well as the call handling application allowing for a flexible, robust and customizable detailed reporting solution. 911 Logix is currently interfaced to log and process the West VIPER®, VESTA® Solutions platforms, Emergency Call Works, Solacom Guardian, Zetron and Frequentis call handling applications.

The platform also has the ability to ingest and report on CAD log files, pre- emergency incident data document (EIDD) format, as well as display weather overlays, Twitter, and Facebook feeds.

911 Logix is an advanced reporting tool that aggregates source data and allows for visualization, reporting, and trending of ESInet content in a Next Generation 9-1-1 (NG 9-1-1) network. The tool produces customizable content and reporting for NG 9-1-1 stakeholders.

Access to the 911 Logix system is available from any device at any time. Users of the system will have near real- time access to the system via VPN and two- factor authentication.

The reporting and data collection system supports multi-tenant role-based access, making pertinent functionality/data available to users based upon permissions. Allowing:

- Statewide users to have access to reports for the entire State.
- Pertinent stakeholders to have both PSAP and ECD Manager level access to report information.
- Pertinent stakeholders to have access to PSAP(s) report information only.

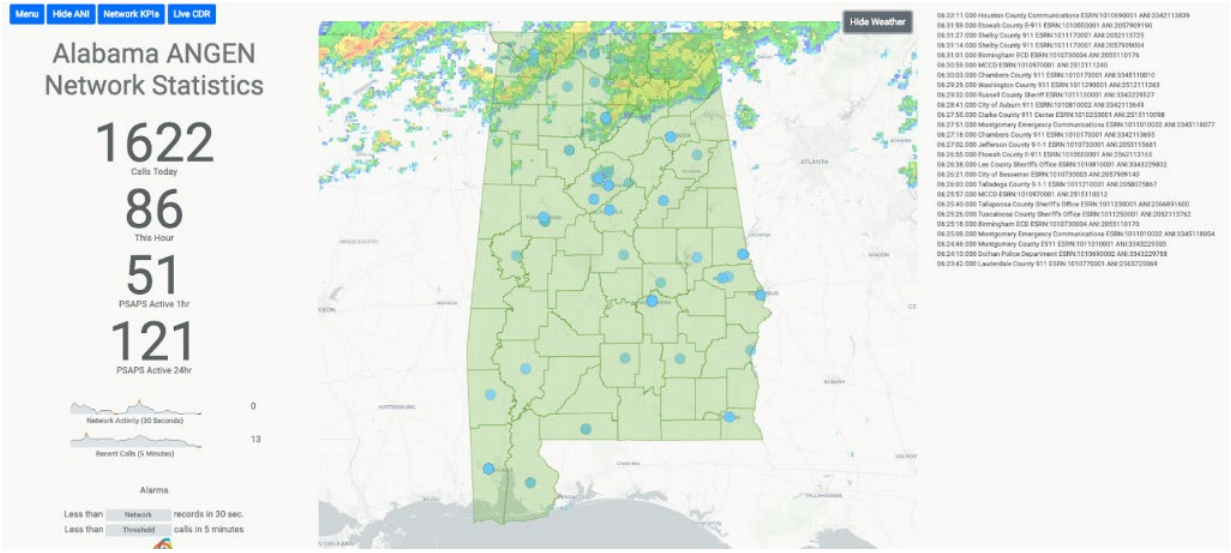
The reporting and data collection system allows for the scheduling of automatic report generation and delivery by email in a customizable format selected by the recipient(s).

911 Logix provides reporting in a tabular fashion on the logs it collects. 911 Logix enables Hamilton, the service provider, as well as the state of Nebraska, to access real-time dashboards. The dashboard(s) create real-time visualizations of activity and performance of the next generation service while also providing for alarming and alerting when deviating from set criteria.

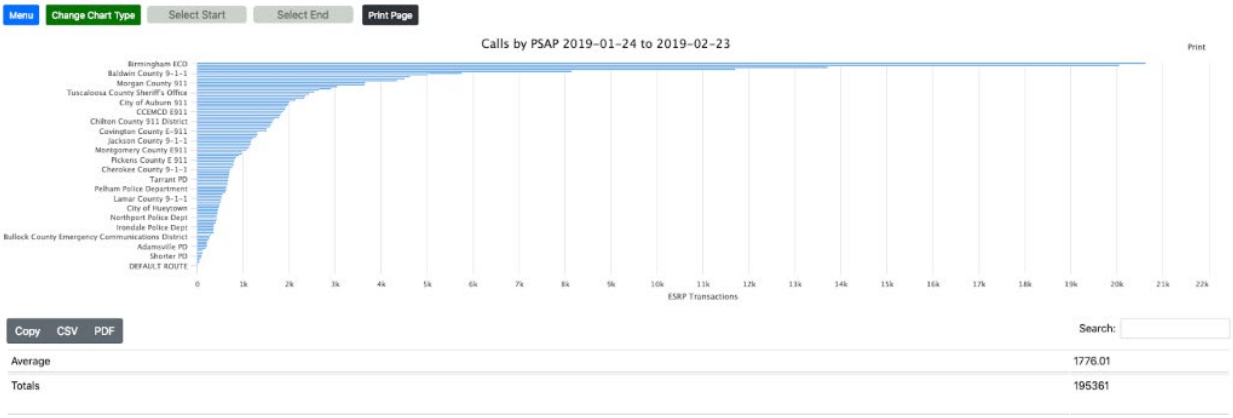
All logging is done with coordinated universal time (UTC) time stamping and converted to the Nebraska local time, based on the user's profile.

The figure below is just one example of a dashboard visualization followed by a sample report.

Sample Dashboard:

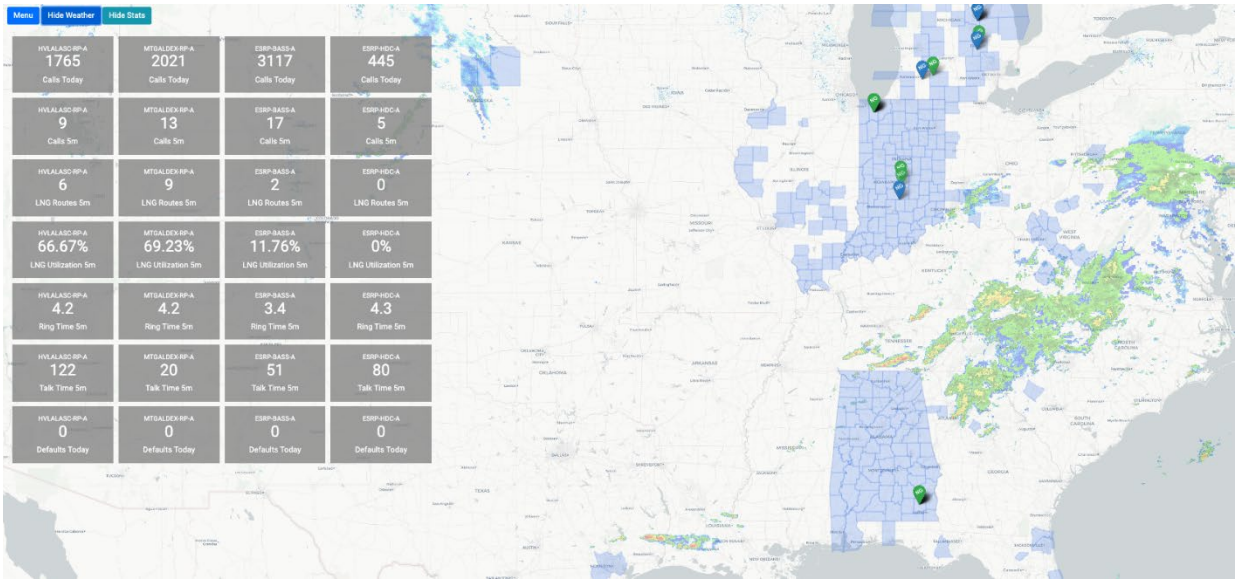


Sample Report:



Hamilton collects event logs from the various network elements (NEs) and functional elements (FEs) in the NGCS core, as well as network events from the tools that are used to surveille and monitor the network. These logged events include ingress and egress to the ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. This enables us to log, display and report on errors. The proposed solution will alert through dashboard visualizations and notification methods.

The example below provides for just one view of a visualization and key performance indicator (KPI) that can be presented based on logs collected at the application and network level.



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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 69.				

Any additional documentation can be inserted here:

Integration with PSAP Call-Handling Equipment

911 Logix has the ability to create ad hoc reports on network or CPE data. Report inquiries that may arise and are not included in the list of standardized reports can be built using the ad hoc reporting tool. Ad hoc reporting allows the end user to query the call database using a set of available query criteria.

Multiple combinations of individual criteria can be used to selectively and efficiently retrieve specific calls or summarize groups of calls. The criteria selection is in a user-friendly format with a drag and drop tool.

Access to Information in the Event-Logging Solution

To use, simply select the variables from the selection on the left side of the screen and drag to the corresponding color column header on the right side of the tool. The resulting data set can then be additionally manipulated using the search function

Requirements of PSAP's Call-Handling Equipment

911 Logix is integrated into the CPE by collecting CDR data from the CPE's controller. CPE from most manufacturers is capable of providing a CDR spill. Depending on the manufacturer, a license to activate that port may be applicable. If a CDR port is not available a CAD spill may be a suitable alternative.

		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: Hamilton complies with requirement NGCS 70.				

Any additional documentation can be inserted here:

Reviewing Recordings/Reports & Retention Periods

Hamilton provides the means for PSAPs and the Commission to gain access to Hamilton's event-logging solution data to run statistical and other MIS reports. Hamilton understands that 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, and 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.

Hamilton will provide access to the dashboards and reports via a centralized command center. The dashboard and associated reports are provided as a suite of products with the tradename "911 Logix." 911 Logix is accessed via a secure dual authentication method provided by "Duo". Once securely logged in, the authorized user can access data and reports via any desktop or mobile device.

911 Logix and all dashboards and visualizations are set up with a hierarchical method so that access to data is controlled by the system administrator. Hamilton will work with the designated technical administrator to determine initial access credentials and

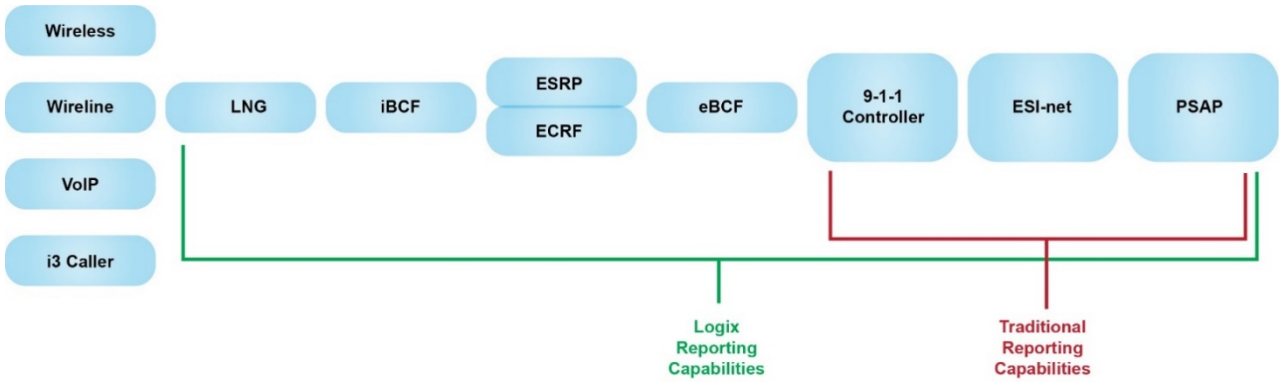
the requirements for password formats and security levels. Once installed, permissions and logon credentials can be self-managed or provided by the Hamilton help desk.

Each of Hamilton's functional elements produce i3 logs. Hamilton will coordinate with ECaTS to provide i3 logs for consumption by ECaTS.

MIS Solution & Required Reports/Metrics

The Hamilton solution includes reports, management information system (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 PSAPs needs. These reports can be utilized for changes to bandwidth and capacity.

To meet this requirement, Hamilton will utilize the appropriate toolset to provide PSAP MIS, network analytics, and visualizations. In addition to providing all required reports, our submission includes numerous dashboards to provide metrics at the PSAP, Regional and Statewide level.

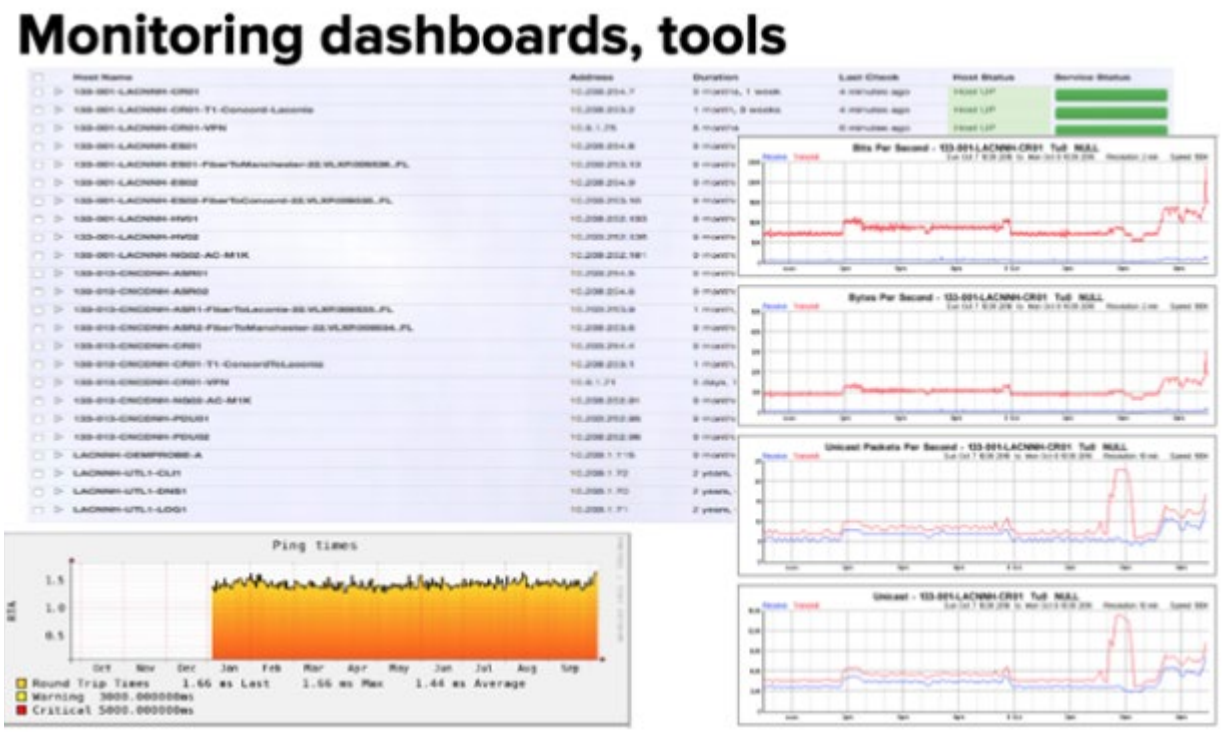


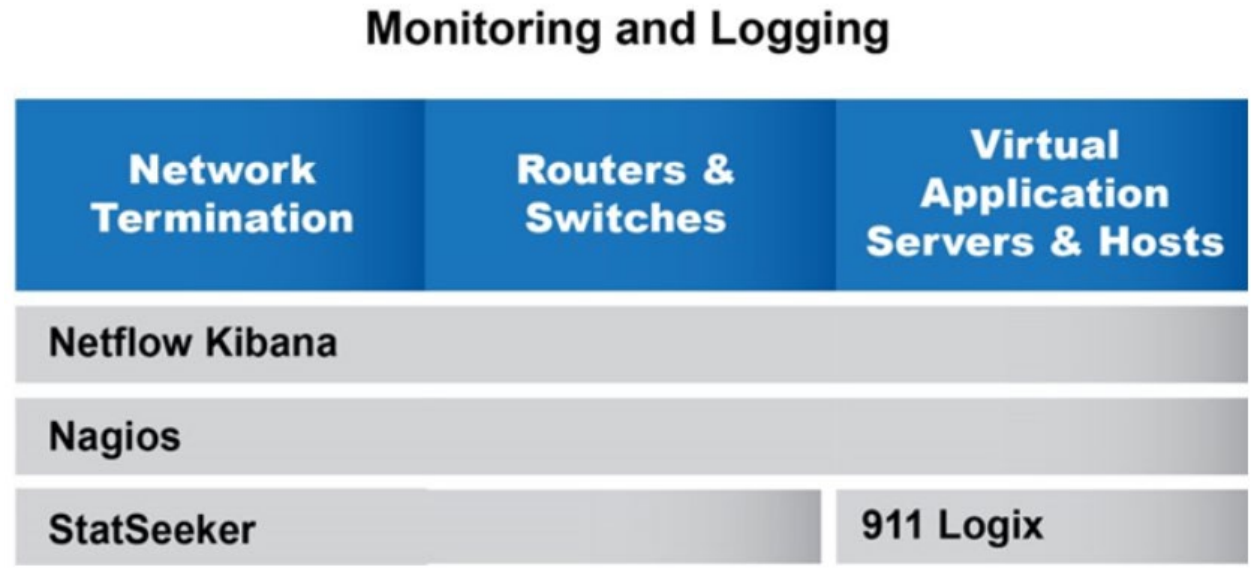
Hamilton uses several platforms for alarms and monitoring of systems (depending on function and system). These network tools include:

- NAGIOS
- Statseeker
- 911Logix
- Logging Subsystem
- Netflow/Kibana
- Forticloud/Fortiview

Dashboards include:

- Providing comprehensive visibility for all systems listed above
- Notifications
- Visual
- Text/ email/ PSNA display





The dashboards and reports are accessed via a centralized dashboard and are provided as a suite of products with the tradename “911 Logix.” 911 Logix is accessed via a secure dual authentication method provided by “Duo”. Once securely logged on, the user can access data and reports via any desktop or mobile device.

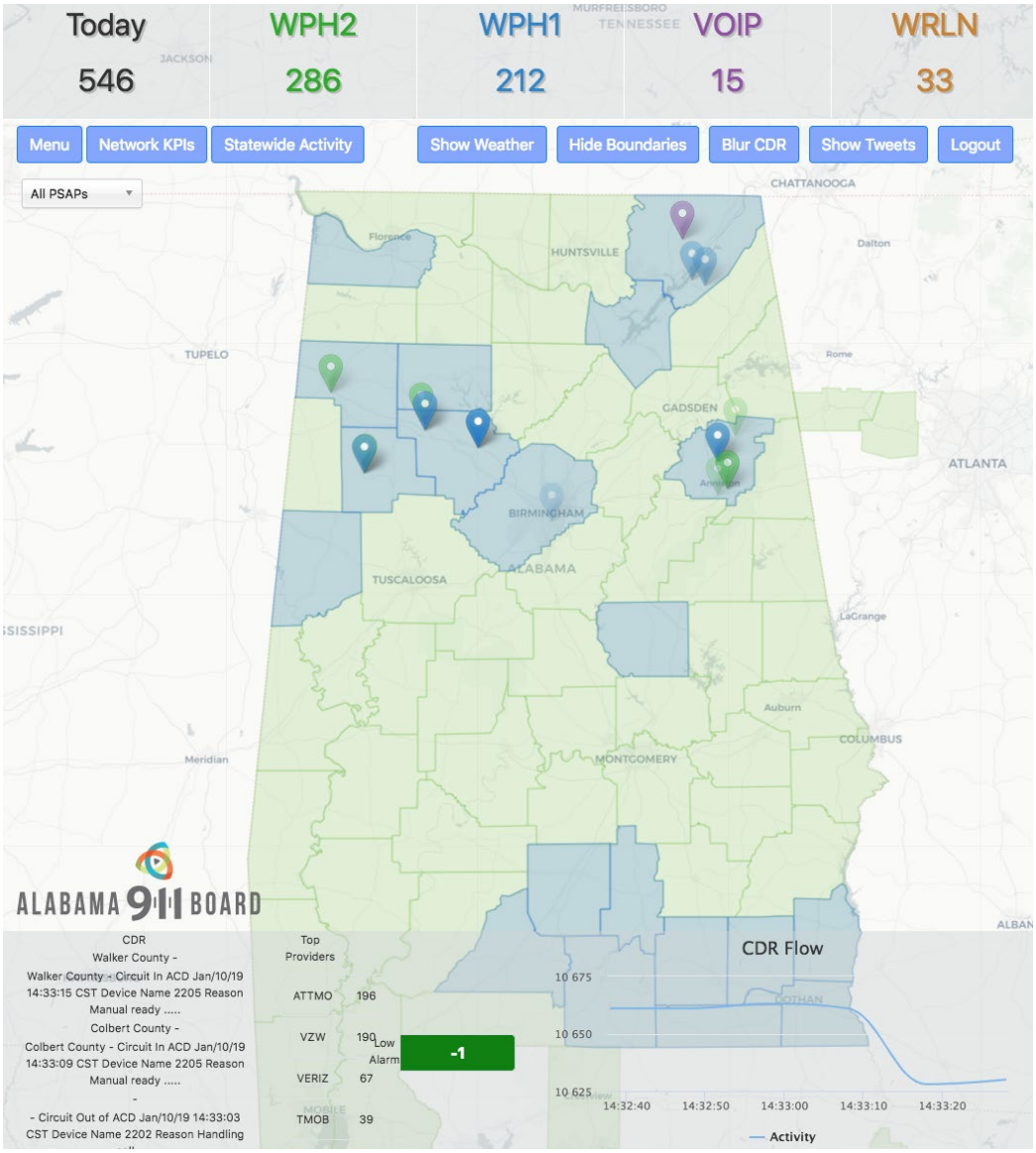
Additionally, new reports are added periodically when users determine that an additional report is required. Our model is predicated on the fact that when a user identifies the necessity for a new report, this report will have utility for other users as well. Therefore, we produce the report and update the 911 Logix system so that all users have access to the report. These new

reports are provided as part of the service. In summary, if the data is available and the user requests a report that can be used by multiple PSAPs, then Hamilton will work with the Commission to produce a new report and make it available to all users.

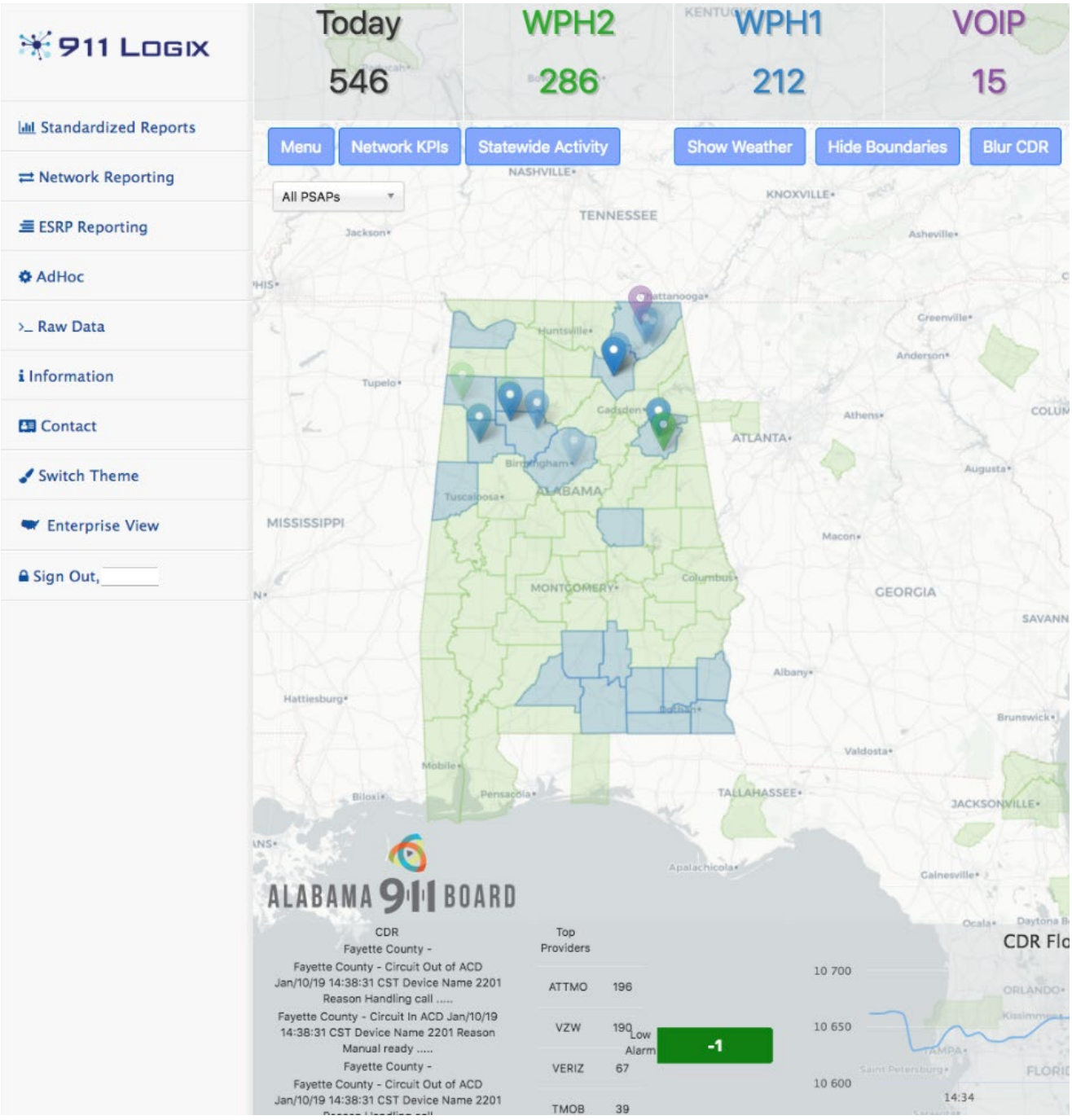
911 Logix and all dashboards and visualizations are set up with a hierarchical method so that access to data is available by permissions. Hamilton will work with the Commission to determine initial access credentials and the requirements for password formats and security levels. Once installed, permissions and logon credentials can be managed as part of the service.

Hamilton will provide standard reports, MIS tools, and performance metrics to be made available to each PSAP and the state of Nebraska monthly or upon request.

Hamilton's reports and metrics will include, but are not limited to, timing, call-delivery time, call-processing time between elements, volumes, call volumes by call type, alternate-routed calls, text-to-911, all NGCS element usage volumes, bandwidth/trunk utilization, calls per trunk, trunk utilization, and circuit utilization. Hamilton has provide some examples of reports below:

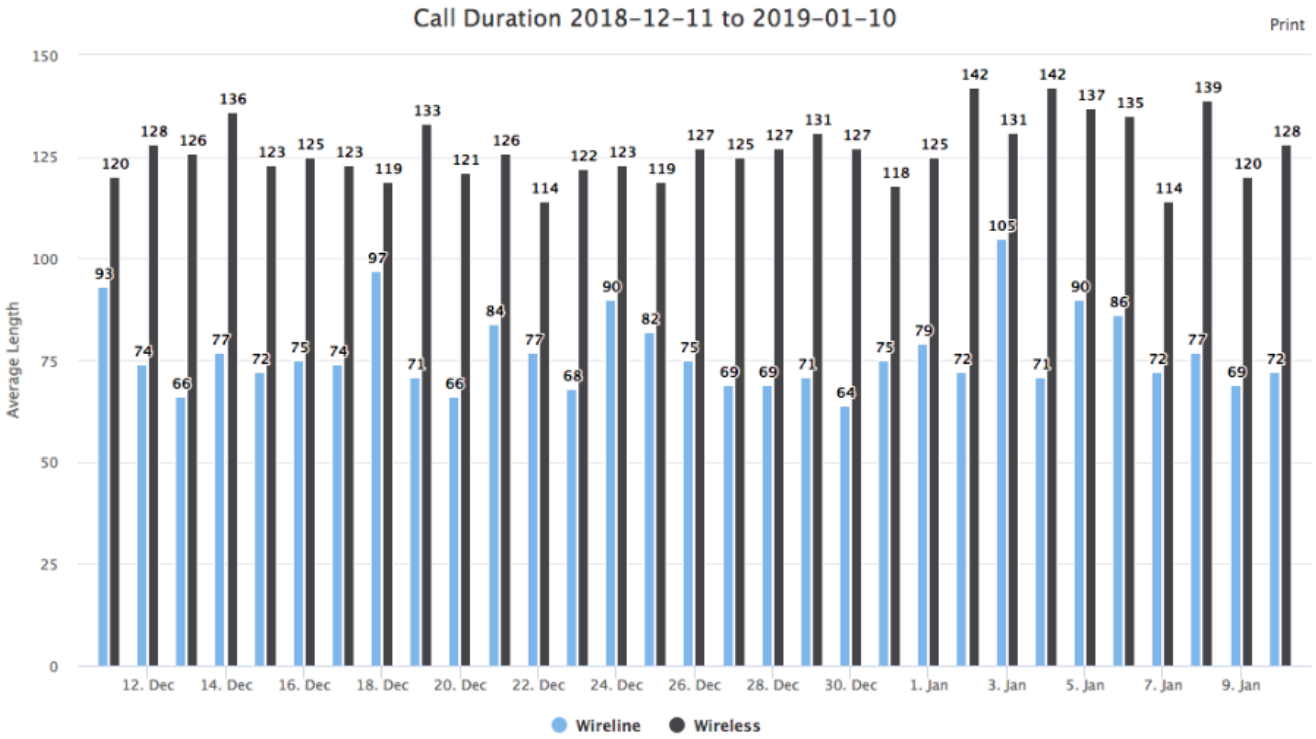


The example above shows the PSAP or Regional interface for tracking 9-1-1 Call Activity and accessing reports.



The example above shows the report interface along the left side of the dashboard displayed when the "menu" button is selected.

Menu | Change Chart Type | Select Start | Select End | All PSAPs | Print Page



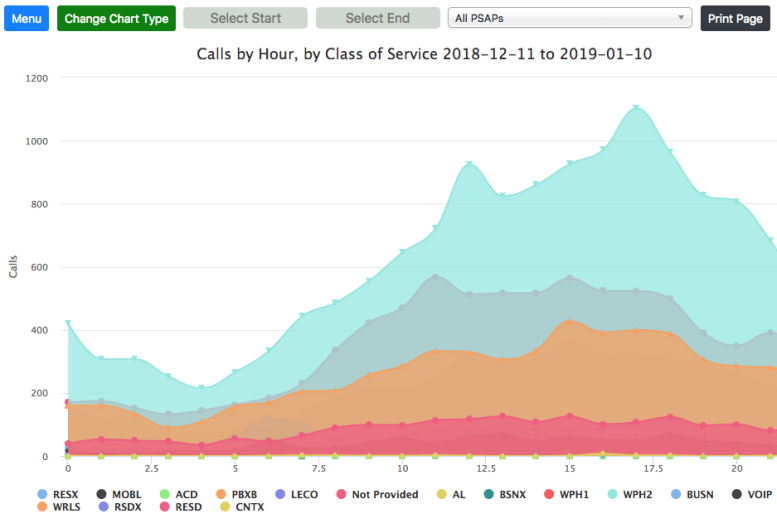
Copy | CSV | PDF

Search:

Average	76.84	126.65

Date	Wireline	Wireless
2018-12-11	93	120
2018-12-12	74	128
2018-12-13	66	126
2018-12-14	77	136
2018-12-15	72	123
2018-12-16	75	125
2018-12-17	74	123
2018-12-18	97	119
2018-12-19	71	133
2018-12-20	66	121

Call Duration



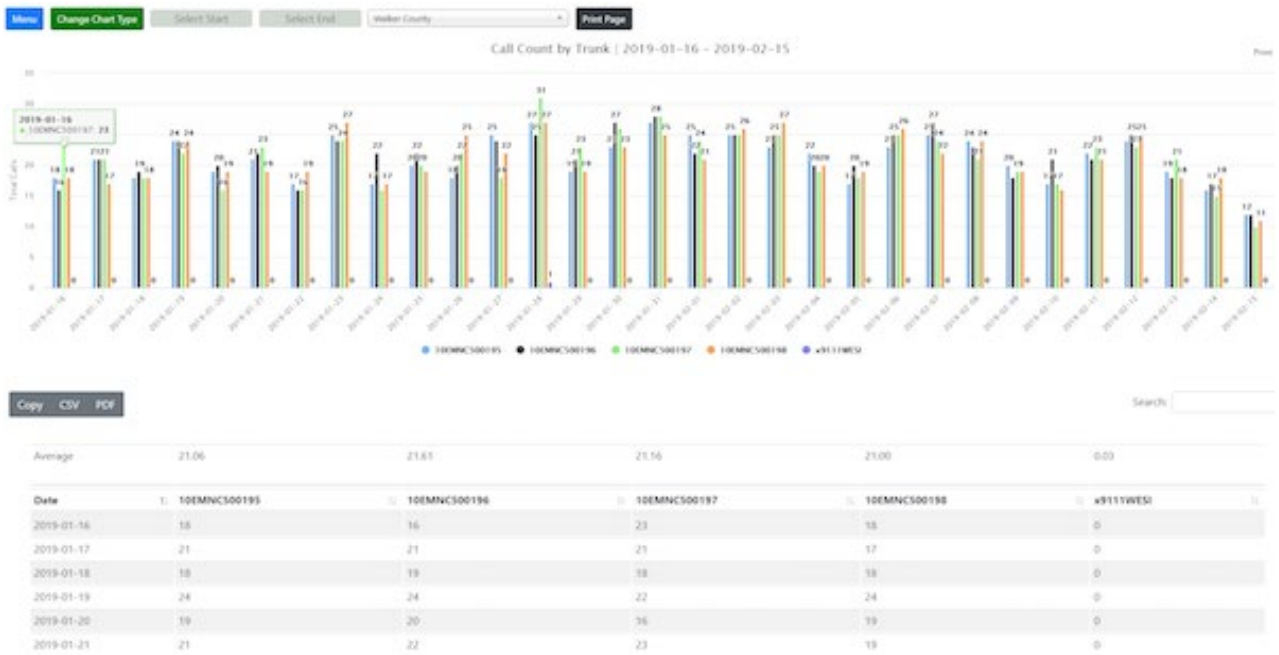
Copy CSV PDF

Search:

Average	28.35	23.81	22.23	17.97	17.45	23.84	28.87	35.39	40.35	48.52	54.32	62.13	68.32
Totals	879 (2.5%)	738 (2.1%)	689 (2.0%)	557 (1.6%)	541 (1.5%)	739 (2.1%)	895 (2.5%)	1097 (3.1%)	1251 (3.5%)	1504 (4.3%)	1684 (4.8%)	1926 (5.5%)	2118 (6.0%)

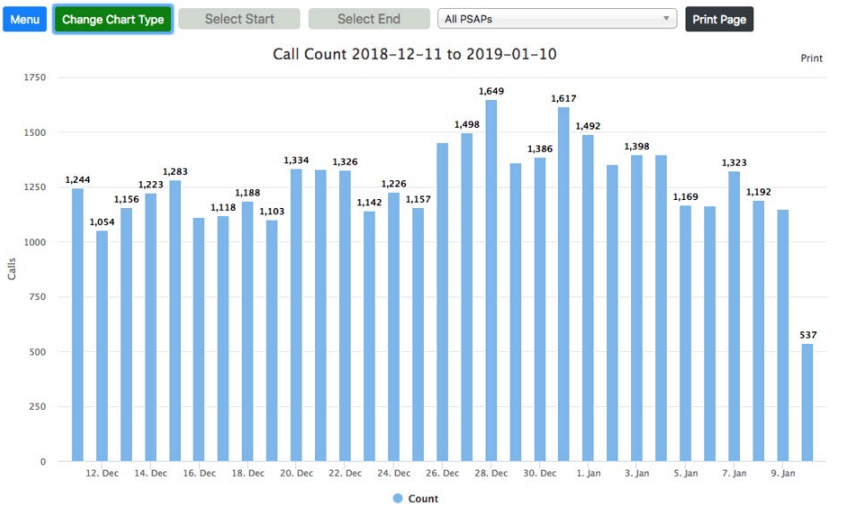
CallDate	0	1	2	3	4	5	6	7	8	9	10	11	12
2018-12-11	24	14	9	22	15	32	25	48	49	53	62	62	60
2018-12-12	20	15	13	13	11	24	37	30	40	38	48	56	43
2018-12-13	18	22	15	20	14	14	35	50	45	56	62	54	69
2018-12-14	22	14	17	13	11	14	26	47	54	41	30	26	59
2018-12-15	29	25	24	8	43	33	24	40	57	43	54	56	92

Call Volumes by Call Type



Call Count by Trunk

Event by Incoming IP Address



Copy CSV PDF Search:

Average	1262.45
Totals	39136 (100.0%)

Date	Count
2018-12-11	1244
2018-12-12	1054
2018-12-13	1156
2018-12-14	1223
2018-12-15	1283
2018-12-16	1111
2018-12-17	1118
2018-12-18	1188
2018-12-19	1103

Total number of wireless and wireline 911 calls answered by State Police PSAPs, by PSAP, by cellular sector, wireline only, wireless only.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 71.				

Any additional documentation can be inserted here:

NENA Standards Compliance

The solution proposed by Hamilton provides a comprehensive logging system and a dual factor secure reporting platform which is accessible via the web portal called 911 Logix. These logs include i3 lots from all ESInet i3 components per the NENA STA-010.2-2016, NENA/APCO-REQ-001.1.1-2016.

Third-Party Certification Fees

Hamilton accepts responsibility for any third-party certification fees associated with event logging.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 72.				

Any additional documentation can be inserted here:

Hamilton's proposed solution achieved time synchronization via network time protocol (NTP). All logging is done with coordinated universal time (UTC) time stamping and is converted to the jurisdiction's local time, based on the user's profile.

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 73.				

Any additional documentation can be inserted here:

Hamilton will provide qualified, source traceable industry standard network time protocol (NTP) servers available for devices that are connected to the ESInet. Hamilton's solution utilizes Stratum 2-time sources and Hamilton will offer PSAPs the use of the NTP service to synchronize the clocks on their 9-1-1 CPE, workstations, etc.

NTP time servers generally transmit Universal Time Coordinated (UTC) and the display device (CPE solution) then displays the selected time zone.

Additionally, Windows 10 can be configured to have the ability to display multiple time zones by clicking the clock in the task bar. Time zones can be named to match local customs and terms. There is no cost for this feature.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 74.				

Any additional documentation can be inserted here:

Hamilton will provide redundant, qualified, source traceable industry standard network time protocol (NTP) servers available for devices that are connected to the ESInet. This will offer PSAPs the use of the NTP service to synchronize the clocks on their 9-1-1 CPE, workstations, etc.

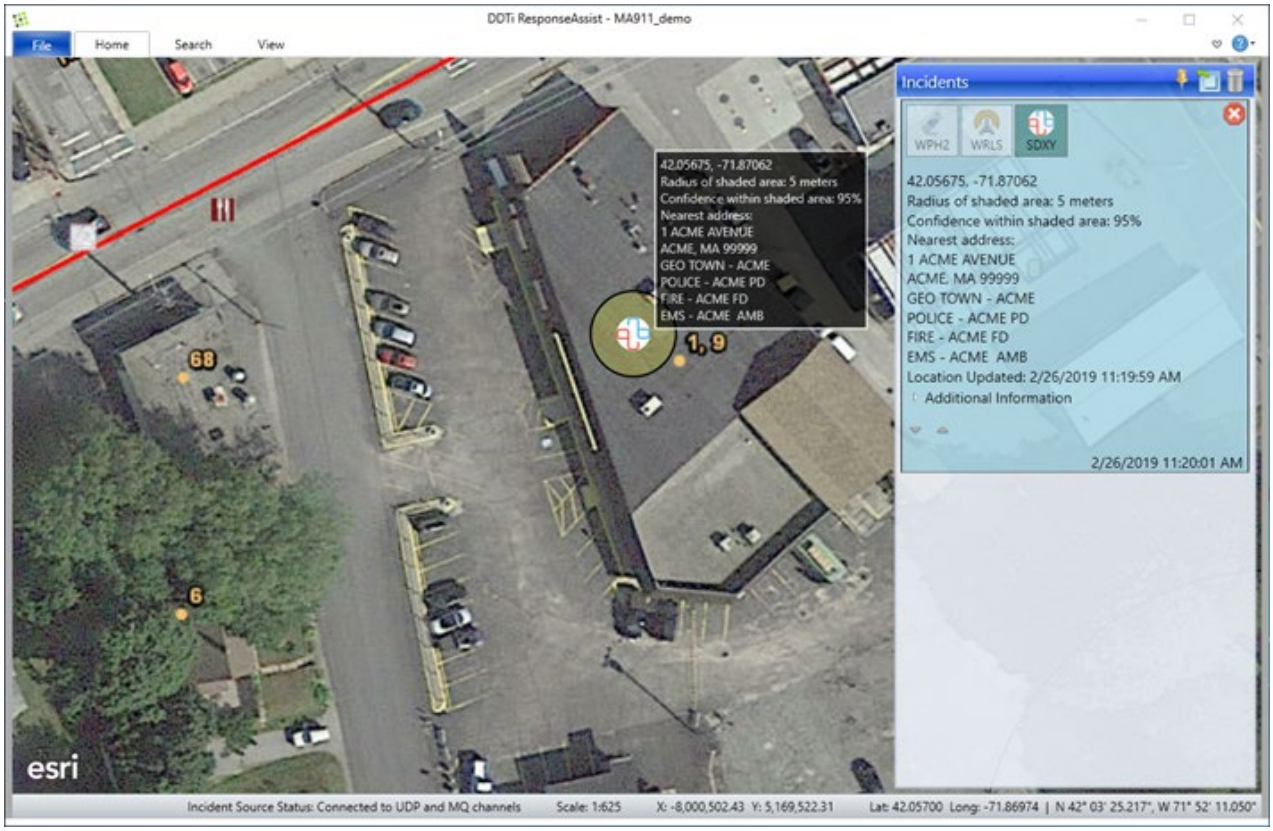
NGCS 75	**Next Generation Core Services Elements (NGCS) NG911 Application Integration** Bidder shall describe other NG911 applications, additional data integrations, and personal safety applications that may be integrated with the NGCS solution. The bidder's system must be capable of integration with 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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with Requirement NGCS 75.				

Any additional documentation can be inserted here:
Hamilton is fully prepared to coordinate integration with many other types of NG 9-1-1 applications, additional data, and personal safety applications. Hamilton is not proposing any specific pricing to facilitate integration. Additional costs will be contemplated and negotiated as needed.

The LDB included in this proposal can act as an ADR out of the box, providing additional data in the HELD response in compliance with IETF RFC 7852 Additional Data Related to an Emergency Call.

Additionally, the LDB can query the external RapidSOS ADR for additional location information for a wireless call. Further development might be needed to support other external ADR's as they become available, particularly if they do not support the HELD protocol.

If the CHE is i3 ready, it should be able to receive PIDF-LO as part of the call payload (or issue a dereference request to the LDB for that information). The LDB will provide all the location information it can to the CHE. The following screenshot shows a call handling tactical map display that has received a PIDF-LO from the LDB with three locations for a single call. The RapidSOS location is shown, with buttons available to switch to the wireless phase I and wireless phase II locations if desired.



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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 76.				

Any additional documentation can be inserted here:

Hamilton provides mature text-to-911 capabilities, which includes the ability to integrate existing web-based and message session relay protocol text (MSRP)-integrated SMS-to-911 and Real Time Text (RTT). These components are included within the Hamilton solution and a distinct differentiator when compared with direct competitors.

Message Session Relay Protocol (MSRP)

Hamilton is a leading provider for non-voice services and support, providing both web-based and direct i3 interface connection arrangements. Hamilton currently operates a text aggregation gateway (TAG) service. This is accomplished by establishing direct network connections to the two primary Text Control Centers (TCCs). Text routing to the ESInet is accomplished by establishing direct connections to the TAG. An alternative VPN connection will also be established to Hamilton's TAG nodes to ensure redundant connections.

Hamilton's text-to-9-1-1 solution does not require any additional applications or software to be installed on a consumer's text-capable device, nor does it require any device to be registered to use the service. Simply stated, any SMS text-capable device

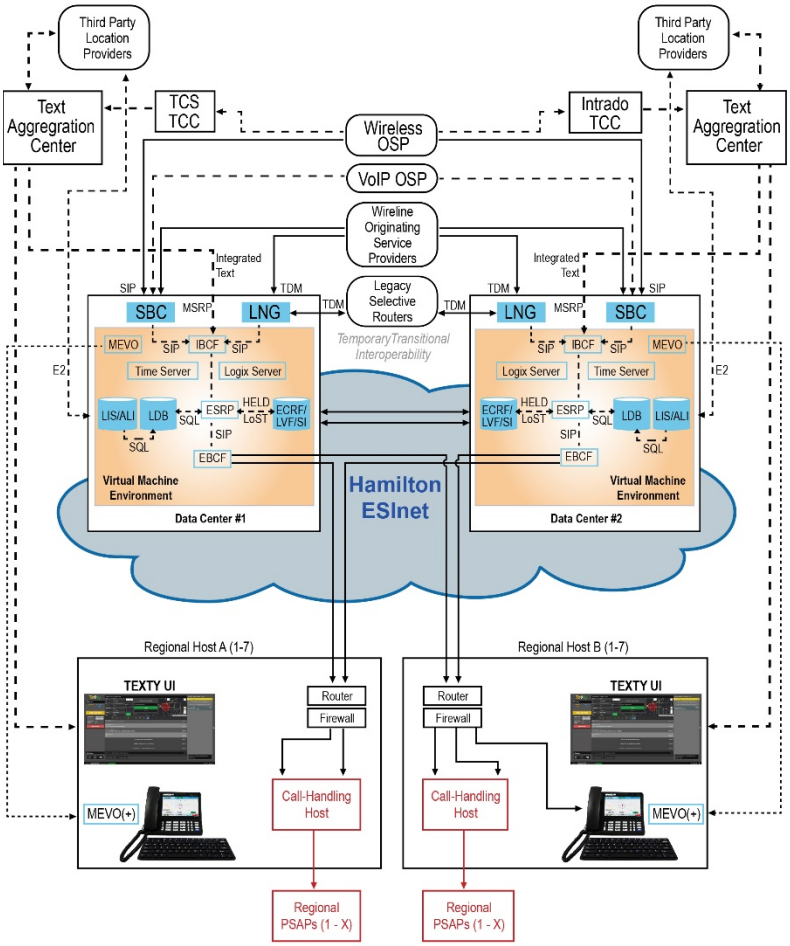
can text to "911" and the text will be delivered to the PSAP. The solution is compliant with the ATIS J-STD-110 standard and all subsequent updates to the standard.

In addition, supported delivery methods to the call taker include Hamilton's web browser platform, Texty, or session initiation protocol message session relay protocols (SIP MSRP) directly to PSAP CHE. Location is conveyed by Geolocation header within SIP signaling of the non-voice payload stream and is therefore fully supported by the IP transport function of the ESInet. While Hamilton supports MSRP, the transition to MSRP for an individual PSAP is solely dependent on the readiness of that PSAP's CPE vendor.

Hamilton's text-to-9-1-1 solution supports the transfer of text sessions between PSAPs. Additionally, the ability to initiate outbound text can be enabled for PSAPs that desire this functionality. This is most commonly accomplished via Hamilton's web browser platform, Texty. Currently, most CPE vendors do not support initiating text sessions directly from the console, but the outbound text service has been integrated into certain compliant 9-1-1 CPE applications.

In addition, Hamilton can provide a text-to-9-1-1 management information system (MIS) package that allows for logging a complete history of text-to-9-1-1 messages and location data. Texty also supports standards-based service enhancements that significantly expand the usefulness of non-voice (text and RTT) based communication for the public and the PSAP.

Additionally, within this proposal, Hamilton is proposing Texty as an optional service to serve as a failover text service, providing enhanced text-to-9-1-1 capabilities for those PSAPs that are already text capable. Additionally, Texty is a web-based option for those PSAPs that are not yet equipped with text-for-911.



Hamilton's network design diagram depicting Hamilton's proposed solution.

Real-Time Text (RTT)

Hamilton recognizes that Real-Time Text (RTT) is an emerging technology that allows individuals to communicate by both speaking and typing text on a phone call and is especially helpful for people who are deaf or who have difficulty in voice-only

communications. RTT enables another way for people to communicate with a PSAP and does replace the need for a PSAP to support text-to-9-1-1. Thus, the transition to RTT from text-to-9-1-1 is something that an individual citizen may choose to do, however Hamilton recognizes that both technologies must be available and supported. The proposed solution supports RTT according to RFC 4103 as outlined in in the NENA i3 spec (NENA STA- 010.2.2016).

Hamilton is at the forefront of the discussion on RTT and strongly believes it serves as a key piece to modernizing 9-1-1 access. In addition, RTT is a significant distinguishing characteristic of the Hamilton solution.

In the past year alone, Hamilton experts have presented on RTT at more than a dozen state-level emergency service conferences, the Federal Communications Commission's PSAP education day, sat on panels for the NG911 Institute, and much more. Hamilton has completed RTT demonstrations for public safety personnel in California, Texas, as well as other states. Hamilton is fully invested in the innovative solution of RTT and the advantages it provides to the emergency communications industry. While RTT is especially helpful for people who are deaf or who have difficulty in voice-only communications, RTT also provides another way for people to communicate with a PSAP.

Unlike text-to-9-1-1, RTT does not involve the use of a TCC, but rather is delivered directly from wireless carriers via an IP interconnection. Hamilton, through its corporate affiliate, Hamilton Relay, a national Telecommunications Relay Service provider, has supported and managed Real-Time Text communications within its IP network since 2011. Hamilton Relay's Traditional 7-1-1 Relay Platform meets the Federal Communication Commission's (FCC) definition of RTT and its associated features and capabilities. Thus, every phone call that Hamilton Relay has processed on its 7-1-1 platform that has involved a TTY has been a successful RTT to TTY call. In the 2019 calendar year, Hamilton Relay answered 2,232,817 calls utilizing Hamilton Relay's Traditional 7-1-1 Relay Platform.

Additionally, for the Hamilton CapTel for business platform, every single HCBIT phone call has used RFC 4103 (i.e. RTT to RTT call) between a customer's CISCO call manager platform (via the "CIS") and Hamilton's Captioning platform (via the "CTIS"). This traffic is 100% real-world experience in delivering RTT to RTT calls.

Overall, Hamilton brings extensive experience in understanding the challenges involved in supporting RTT, as well as an understanding of the needs of individuals who are deaf, hard of hearing or who have other accessibility needs. These individuals will most likely be the early adopters of RTT. For these reasons, Hamilton is in a uniquely qualified position to deliver early availability of this technology to the state of Nebraska.

Once RTT capable cellular OSPs are aggregated to the ESInet, Hamilton can deliver RTT in a native format to the PSAP or convert the RTT to MSRP format. As part of the deployment, Hamilton can deploy RTT to every telecommunicator in the state utilizing the optional MEVO(+) platform. In the event of a service impairment, MEVO(+) can serve as a failover solution, ensuring that a public caller will reach the PSAP. MEVO(+) allows the call taker to continue normal operations with a high level of functionality, including the ability to view all automatic location identification (ALI) information and perform rebids for updated location information.

NGCS 77	**Next Generation Core Services Elements (NGCS)** **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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
	Bidder Response: Hamilton complies with requirement NGCS 77.				

Any additional documentation can be inserted here:

Make-Busy Functionality

Most failover mechanisms are triggered automatically through the policy routing function (PRF). An alarm is sent to the network operations center/security operations center (NOC/SOC) when a call is delivered using a secondary or tertiary PRF destination. NOC/SOC technicians investigate each of these alarms for further evaluation or mitigation.

Hamilton's proposed solution includes multiple ways to access the PRF, which is the functional element to reroute 9-1-1 traffic if necessary. Re-routing calls can be accessed via web interface, the MEVO(+) phone Optimal Service Button (OSB) button, or by calling Hamilton's NOC/SOC.

Failovers can also be triggered manually. For example, using the OSB, the PSAP can activate an abandon PSAP scenario or "make busy" switch for the PSAP. The OSB forces the PSAP's calls to a second destination as directed by the PSAP. Activation of the OSB also triggers an alarm at the NOC/SOC and technicians will contact the PSAP to provide any needed assistance.

A third option for failovers is to simply contact the NOC/SOC and request that calls be redirected. This is a preferred approach in a non-emergency situation. Contacting the NOC/SOC allows the NOC/SOC to make test calls and confirm everything is working as it should.

Ringdown Functionality

Hamilton's proposed solution can support the Ring-Down functionality requirement desired by the Commission. While this is primarily done from the legacy network gateway (LNG), Hamilton can also support this functionality through the emergency service routing proxy (ESRP). Hamilton will work collaboratively with the Commission to ensure this functions as the state desires.

Near-Simultaneous Transfer

Most often, the conference requirement is a capability of a hosted call handling equipment (CHE) solution. However, next generation core services (NGCS) core is equipped to allow multiple parties to be added in a single "Add Party" request. It will allow for the configuration of up to 50 multi-party entries. Each entry is designated by a SIP URI so the call handling system can identify it in an Add Party request. Each multi-party entry will allow up to 10 SIP URIs which identify the parties to be added to a call.

If the optional MEVO(+) failover platform is placed into operation, MEVO(+) will also support Multi Party Conferencing.

To support PSAP to PSAP transfers with the legacy selective router (LSR) during the transitional stage of the project, the LNG and LSRG serve as signaling and media interconnection points between callers in the legacy originating networks and the proposed Hamilton ESInet. The LNG's purpose is to convert calls from time division multiplexing (TDM) to session initiation protocol (SIP) signaling for ingress to the ESInet. The LSRG converts calls from SIP to TDM signaling for egress from the ESInet to the legacy selective router.

To enable calls to be routed and/or transferred and/or handed-off between legacy and the Hamilton next generation emergency network, the legacy LSRG will provide an interface between a 9-1-1 selective router and the ESInet.

Furthermore, Hamilton has developed a specialized functional element (FE) appliance to support legacy star code transfers via a conversion to SIP messaging. This FE appliance is named HFA and is deployed throughout our service footprint. We also support the conversion of SIP transfer messaging to star codes for integration of NG PSAPs to legacy E9-1-1 networks.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 78	**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.	X			
	Bidder Response: Hamilton complies with requirement NGCS 78.				

Any additional documentation can be inserted here:

All functional elements support RFC-3261 and related RFCs for handling SIP based communications. This provides for the baseline interoperability with NG 9-1-1 PSAPs using SIP. Additionally, all pertinent functional elements support the dereference and call routing resolution protocols based on i3 identified RFCs used for a HELD, AD, and LoST implementation within the NGCS.

All medias that can be negotiated in service delivery platform (SDP) are supported within the NGCS. This is due to the nature of our NGCS functional elements (FE), as they do not necessarily process media unless required by the job they fulfill in real time. This is considered a media-flow-around model. We use 3PCC and rehome media to appropriate media-anchors when needed throughout the life of a call. For example, the Conference Focus Function within the BCF only uses Media-Resource Functions when Transfer or Conference is requested. These resources are shared and freed once no longer in use. The Media resources are deployed redundantly, shared, and invoked only on a per need basis. This is very similar to IP-multimedia subsystem (IMS). There are, however, a couple of places within the call chain where we do anchor the media on purpose for all calls. One is at the border of neighboring networks. We use SBC(s) that will police and anchor the media for security, topology hiding, and traffic engineering purposes. Today, these SBCs are based on a robust OTS model that support the primary media types needed for NG 9-1-1. But, the ESInet is not limited to only these medias in practice.

Regarding discrepancy reporting, Hamilton currently has on its roadmap to support discrepancy reporting from certain key FEs and will do what it can to abide by the requirements of the project. At this time, Hamilton does have the capability to report some discrepancies, including event logging, default-routed, no record found, etc. To provide a full discrepancy function, custody and alerting must be components and Hamilton will work with the Commission to provide the functionalities necessary to fulfill the requirements of the contract. Additionally, it's important to note that NENA committees are actively discussing discrepancy reporting and how it is defined and supported.

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.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 79.				

Any additional documentation can be inserted here:

Implemented CHE Platforms

The ESInet solution proposed by Hamilton supports NENA i3, intermediate transitional SIP, T-1 and reverse battery centralized automatic messaging accounting (CAMA), multi-frequency T-1 interfaces, and primary rate interface (PRI) options. This provides full support for hosted systems, with the full flexibility within the Nebraska NG 9-1-1 network. This flexibility removes all barriers to participation, regardless of the age or capabilities of the PSAP CPE or other equipment. Hamilton is successfully interconnected with the following NENA i3 compliant CPE vendors:

- Motorola VESTA® Solutions
- Solacom Guardian 9-1-1 Call Handling
- Motorola Emergency CallWorks Solution (ECW)
- Intrado VIPER®
- Zetron
- Moducom
- Frequentis

Hamilton has tested and has in-production ESInet to CPE integration with all major 9-1-1 CPE manufacturers listed above. This includes most current production releases from all listed vendors.

Testing Process

For equipment that has not yet been tested at a NENA ICE events, Hamilton has either completed lab review and compliance testing, or it is in the marketplace with an established production history. Hamilton requires compliance testing before the equipment is put into production. This testing process will follow established industry standards, and the results will be made available to the Commission for review.

Physical Interface Handoff

The physical interface handoff required at the Regional Call Host (RCH) demarcation point includes a pair of Cisco routers. The routers can accommodate either optical or ethernet connections and Hamilton will accommodate the existing or desired interface of the RCH equipment.

NGCS 80	**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 X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Hamilton complies with requirement NGCS 80.				

Any additional documentation can be inserted here:

Hamilton's proposed solution supports the forwarding of 9-1-1 calls to the public switched telephone network (PSTN). With the appropriate configuration, the ability to query location can occur when the call has been forwarded to the MEVO(+) failover

platform. The location information can only be queried when the OSP makes call back number (CBN) information available in the incoming SS7 signaling data. Not all OSPs provide this SS7 configuration and rely on their third-party providers for the CBN. For those carriers that do not provide the SS7 configuration, the call back number is available from a query place by the legacy automatic location information (ALI) sub-system and will be logged in the i3 logging functional element (FE).

SVAL-1	**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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement SVAL-1.				

Any additional documentation can be inserted here:

Hamilton willingly complies with this requirement and will actively work with the service authority to ensure there are no issues in validating Hamilton's solution.

OPTIONAL SERVICE

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Hamilton complies with requirement NGCS 81.				

Any additional documentation can be inserted here:

Hamilton's proposed solution supports the integration of alarm and sensor data within the next generation core services (NGCS). Further, supplemental third-party data can be accepted by the network through the use of an application programming interface (API). Hamilton's network solution has been tested extensively with third-party data providers, such as OnStar, along with many others. Hamilton is committed to working with alarm companies and third-party data providers who are ready to establish an IP based interconnection to the network.

HAMILTON APPENDIX 1: HAMILTON NG911 PRE-QUALIFICATION BOND LETTER

CNA SURETY

June 1, 2020

State of Nebraska
Attn: Annette Walton and Nancy Storant
1526 K Street, Suite 130
Lincoln, NE 68508

Re: Hamilton NG911,Inc.
Bond Amount: $500,000

Dear Ms. Walton and Ms. Storant:

This letter is being written at the request of Hamilton NG911, Inc. as part of the pre-qualification process. Bonds for Hamilton are written by Western Surety Company, a CNA Surety writing company.

Hamilton has or is about to submit a proposal for Next Generation 911 Emergency Services IP Network and Core Services. If a contract is awarded to Hamilton, it is our present intention to become surety on the performance bond and labor and materials bond required by the contract.

Any arrangement for bonds required by the contract is a matter between Hamilton and the surety and we assume no liability to you or your third parties, if for any reason we do not execute these bonds.

Sincerely,

Joan Leu
Attorney-in-fact
Western Surety Company

CC: Hamilton NG911, Inc.

HAMILTON APPENDIX 2: CERTIFICATE OF INSURANCE/ ACORD FORM (COI)

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 5/28/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER UNITEL 1128 Lincoln Mall Suite 200 Lincoln, NE 68508	**CONTACT NAME:** UNITEL **PHONE (A/C, No, Ext):** 402-434-7255 **FAX (A/C, No):** 402-434-7272 **E-MAIL ADDRESS:**
	INSURER(S) AFFORDING COVERAGE / **NAIC #** **INSURER A :** Hartford Insurance Company **INSURER B :** The Travelers Indemnity Company **INSURER C :** **INSURER D :** Axis Insurance Co. **INSURER E :** **INSURER F :**
INSURED Hamilton NG911, Inc. 1006 12th Street Aurora NE 68818	

COVERAGES **CERTIFICATE NUMBER:** 55697835 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	✓ **COMMERCIAL GENERAL LIABILITY** ☐ CLAIMS-MADE ✓ OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: ✓ POLICY ☐ PRO-JECT ☐ LOC ☐ OTHER:			91UUNND6927	6/30/2019	6/30/2020	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 500,000 $ 10,000 $ 1,000,000 $ 3,000,000 $ 2,000,000
A	**AUTOMOBILE LIABILITY** ✓ ANY AUTO ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS ✓ HIRED AUTOS ONLY ✓ NON-OWNED AUTOS ONLY			91UUNND6927	6/30/2019	6/30/2020	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ 1,000,000 $ $ $
A	☐ **UMBRELLA LIAB** ✓ OCCUR ✓ **EXCESS LIAB** ☐ CLAIMS-MADE ☐ DED ✓ RETENTION $ 10,000			91RHUNDO918	6/30/2019	6/30/2020	EACH OCCURRENCE AGGREGATE	$ 20,000,000 $ 20,000,000
B	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? ☐ **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		UB-7K93643A	6/30/2019	6/30/2020	✓ PER STATUTE ☐ OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
D	Technology Error & Omissions			P-001-000025066	6/30/2019	6/30/2020	$10,000,000	
D	Errors & Omissions			P-001-000025066	6/30/2019	6/30/2020	$1,000,000	
A	Crime/Employee Dishonesty			91KB0296846	6/30/2019	6/30/2020	$1,000,000 - includes 3rd party	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Names below are listed as an Additional Insured with respect to General Liability on a Primary and Non-contributory basis. A Waiver of Subrogation applies to General Liability and Workers Compensation. RFP #6264 Z1
INdigital, GeoComm, DDTI, NebraskaLink

CERTIFICATE HOLDER

Public Service Commission
Attn: State 911 Director
PO Box 9427
Lincoln NE 68509

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Shane Ideus

HAMILTON APPENDIX 3: THE ECONOMIC IMPACT OF HAMILTON'S NEXT GENERATION 9-1-1 ON NEBRASKA

The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska

Prepared for: Hamilton Telecommunications

May 27, 2020

Goss & Associates Economic Solutions
Ernest Goss, Ph.D., Principal Investigator
Scott Strain, Senior Economist
600 17th Street, Suite 2800 South
Denver, Colorado 80202-5428
303.226.5882
www.gossandassociates.com

Goss & Associates

A VETERAN OWNED FIRM

Table of Contents

The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska

Preface

The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska

This analysis was prepared for Hamilton Telecommunications. Findings remain the sole property of Hamilton Telecommunications and may not be used without prior approval of this organization.

This report was produced independently by the principal investigators. Any errors or misstatements contained in this study are solely the responsibility of the authors. Please address all correspondence to:

Dr. Ernest Goss,[1]
Principal Investigator
MacAllister Chairholder
Department of Economics
Creighton University
Omaha, Nebraska 68178-0130
ernieg@creighton.edu
Voice-(402) 280-4757
Fax-(402) 280-2172
www.gossandassociates.com

Scott Strain, MS
Co-Principal Investigator
Goss & Associates, Economic Solutions
Scott.strain@gossandassociates.com

May 1, 2020

[1] A copy of the principal investigators' biography is contained in Appendix H.

Executive Summary

The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska

Overview: Assuming that Hamilton is awarded, for example, a five million dollar contract for Next Generation 911 (hereafter NG 9-1-1), it is concluded that one year of operations will generate $9,403,539 in total impacts, $4,178,457 in wages & salaries, and $421,743 in self-employment income for the State of Nebraska for year one.[2] Furthermore, it is estimated that this five million dollar contract will produce $354,779 in state and local taxes. These economic impacts are almost double that furnished by out-of-state competitors.

By applying Hamilton's expected investment in NG 9-1-1 supporting payroll and revenue data for year one operations in Nebraska to Input-Output models,[3] it is estimated that Hamilton's NG 9-1-1 in-state center will produce the following direct and indirect contributions to the State of Nebraska:

I. To the Local and State Economies

- Hamilton's in-state NG 9-1-1 services contract spending will add an estimated $9.1 million to the Nebraska economy for year one operations.[4] This compares to a much smaller $5.0 million impact for an out-of-state provider.

II. To State and Local Tax Collections

- For year one, it is estimated that Hamilton's NG 9-1-1 operations will generate $354,779 in **state and local taxes**. This compares to a much smaller $129,425 for a non-Nebraska competitor.

III. To the State 's Labor Force

- For year one, Hamilton NG 9-1-1 operations will support 146 jobs in the economy with a total payroll of approximately $4,178,457[5]. This compares to a much lower 102 jobs with total payroll of $2,760,016 for an out-of-state competitor.
- For year one, Hamilton NG 9-1-1 operations will support $421,743 in self-employment income for entrepreneurs in Nebraska. This compares to a much lower $242,649 for an out-of-state competitor.

For year one, it is estimated that Hamilton's NG 9-1-1 operations will generate $354,779 in state and local taxes. This compares to a much smaller $129,425 for a non-Nebraska competitor.

[2]Unless stated otherwise, all financial data are in 2020 dollars.

[3]This study was completed using regional impact multipliers from IMPLAN, Inc. IMPLAN'S methodology is contained in Appendices A-F. The term "Hamilton" used throughout refers to both Hamilton Telecommunications and its subcontractors.

[4]Approximately $4.2 million of this impact represents spillover impacts. Spillover impacts represent 'ripple' impacts in related businesses as the initial contract dollars are re-spent in the community. For example, Hamilton Telecommunications workers will spend a portion of their earnings in local grocery stores. This spending creates sales, earnings and jobs, termed spillover impacts, for businesses in the retail trade sector..

[5]Hamilton compensation includes fringe benefits and FICA taxes paid by the employer on behalf of the employee. These costs are estimated to be approximately 30% of the compensation value. Hamilton provides a comprehensive benefit plan which includes company paid health and life insurance, long term disability insurance, section 125 cafeteria plan, 401(K) and paid time off.

Executive Summary

IV. To a Stable Job Base

- Hamilton NG 9-1-1 will have a stabilizing impact on the local economy with the number of jobs provided by the contract likely to remain stable, or increase over the period of the contract.
- Since 1901, Hamilton has been a significant contributor to Hamilton County and Nebraska economic development. For example, the firm's growth has expanded by 11 times that of the Nebraska economy and 20 times that of the Hamilton County economy.
- As a result of Hamilton's long and successful Nebraska operations, backward linkages to suppliers and forward linkages to purchasers, are well-developed, enhancing long-term economic impacts.

Since 1985, Hamilton has been a significant contributor to Hamilton County and Nebraska economic development. For example, the firm's growth has expanded by 11 times that of the Nebraska economy and 20 times that of the Hamilton County economy.

V. To Nebraska's Economic Growth

- The award of this contract to an out-of-state competitor would mean that the revenue from this contract would go to another location and state with resultant job losses for the Nebraska and Hamilton County economies.
- These lost dollars, which would be "new" to the county are particularly important in generating new jobs and economic growth for the state and rural Hamilton County[6].
- Every dollar of the Hamilton NG 9-1-1 contract produces $1.89 of impacts for the Nebraska economy.
- This large impact is due to the fact that Hamilton supports services for other states from their Nebraska suppliers. Figures 1, 2 and 3 summarize and compare NG 9-1-1 economic impacts from Hamilton versus non-Nebraska competitors.

Every dollar of the Hamilton NG 9-1-1 contract produces $1.89 of impacts for the Nebraska economy.

As a result of Hamilton's long and successful Nebraska operations, backward linkages to suppliers and forward linkages to purchasers, are well-developed, enhancing long-term economic impacts.

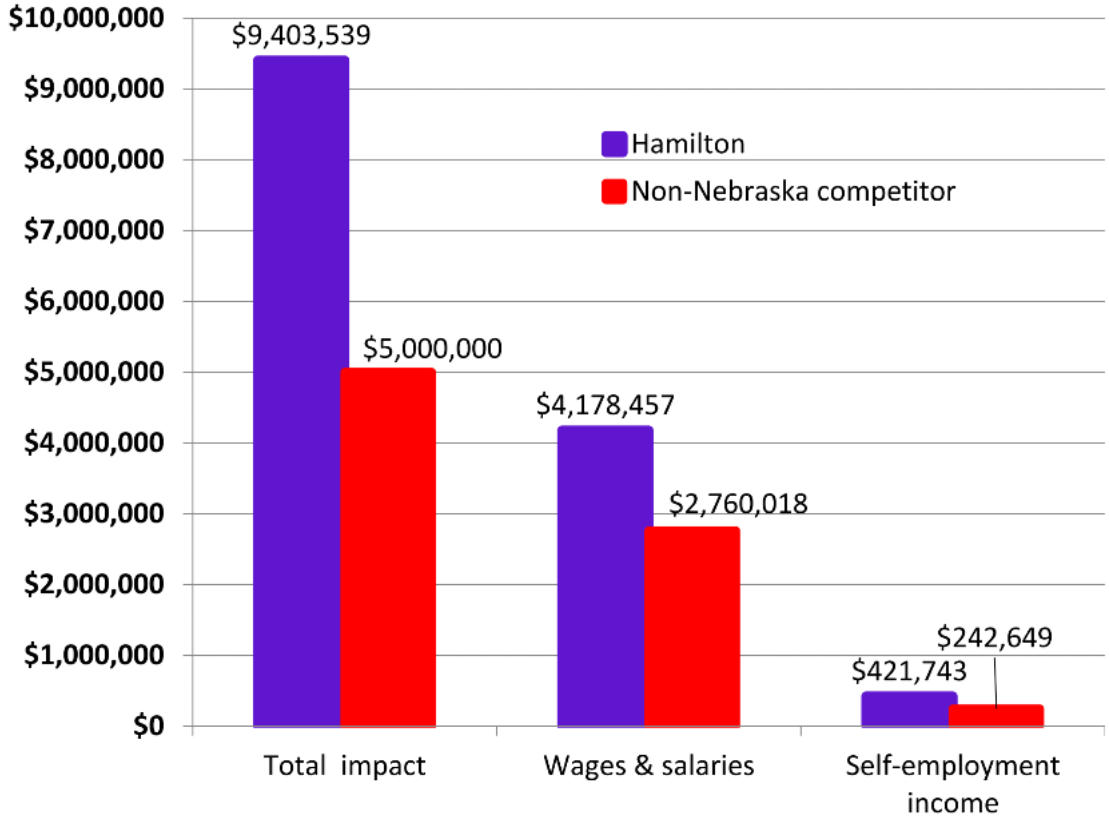
[6]Goss & Associates anticipates that the award of the Nebraska contract to another bidder could cause the bidder to service customers from another state.

Executive Summary

F igures 1, 2, and 3 summarize and compare NG 9-1-1 economic impacts.

Figure 1 lists total impacts for year one of the contract. This indicates that every dollar of the NG 9-1-1 contract results in nearly $1.88 of Nebraska impacts. This large ratio is due to the significant supply chain relationships maintained by Hamilton Telecommunications as a result of the provision of telephone services to other states from the Nebraska location.

Figure 1: Economic impacts, Hamilton vs. Non-Nebraska firm, year one

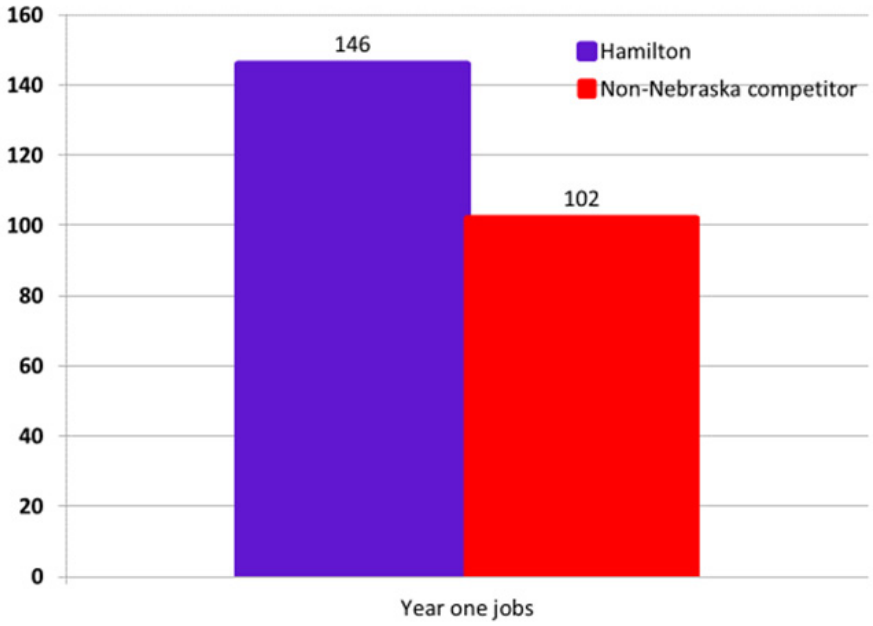


Source: Goss & Associates, 2018, based on IMPLAN Multipliers

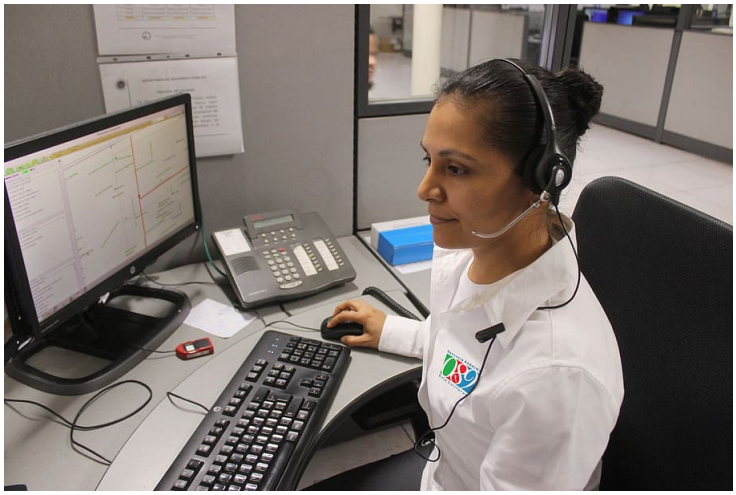
Executive Summary

Figure 2 compares NG 9-1-1 job impacts for Nebraska between Hamilton and non-Nebraska competitors of the NG 9-1-1 contract. As profiled, each $1,000,000 of NG 9-1-1 contract produces approximately 29 jobs in the economy from Hamilton operations and 20 jobs from non-Nebraska competitors. The jobs impact is based on a $5,000,000 contract example.

Figure 2:Job impacts, Hamilton vs. Non-Nebraska firm, year one



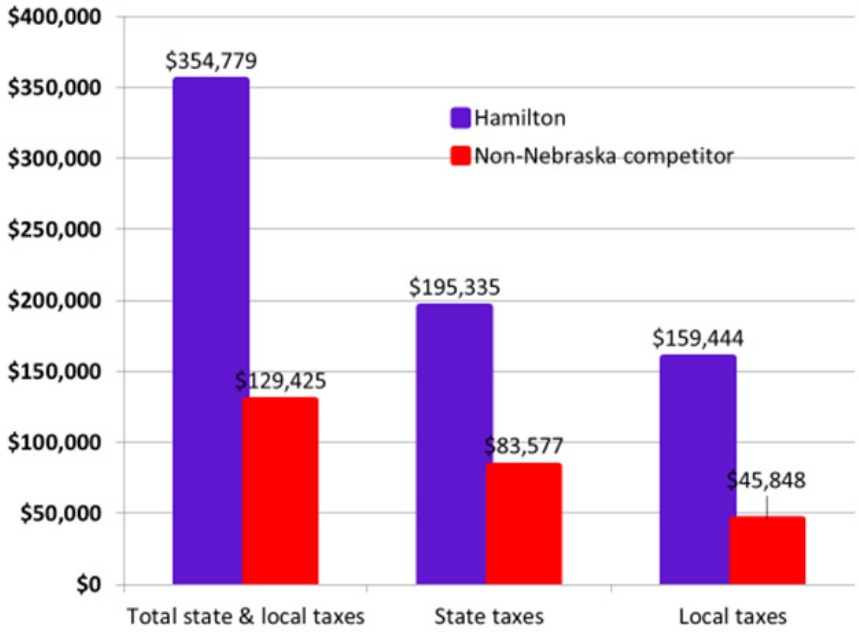
Source: Goss & Associates, 2018, based on IMPLAN Multipliers



Executive Summary

Figure 3 shows state and local tax impacts from Hamilton NG 9-1-1 operations, versus non-Nebraska competitors. As presented, Hamilton operations will generate $354,779 in state and local taxes compared to a lower $129,425 for out-of-state competitors.

Figure 3: State & local tax impacts: Hamilton vs. Non-Nebraska firm, year one



Source: Goss & Associates, 2018, based on IMPLAN Multipliers

Executive Summary

Table 1: Summary of annual economic impacts of NG 9-1-1 contract on the Nebraska County economy			
	Year one Total		
	Hamilton	Out-of-state competitor	Reference
Annual impact on Nebraska County economy	$9,403,539	$5,000,000	Table 3, page 9
Annual impact on wages & salaries	$4,178,457	$2,60,018	Table 4, page 10
Self-employment income	$421,743	$242,649	Table 5, page 11
Jobs supported by contract spending	146	102	Table 6, page 12
Annual Impact on state and local tax collections	$354,799	$216,992	Table 7, page 12
Source: Goss & Associates based IMPLAN Multipliers, 2020			

The Economic Impact of Hamilton's Next Generation 9-1-1 on Nebraska

Introduction

Goss & Associates was asked by Hamilton Telecommunications to estimate the year one economic impacts of the proposed NG 9-1-1 contract on the State of Nebraska[7]. The estimates that follow use initial business and area conditions listed in Table 2, and the methodology described in the accompanying appendices.

Tables 3, 4, 5, 6 and 7 provide detailed estimated impacts. Estimates indicate that the impacts are broadly dispersed with all of Nebraska's major industry sectors experiencing economic impacts, either directly or indirectly, from the NG 9-1-1 contract.

The economic impacts identified in this study are short-run in nature and represent annual, recurring events, but will expand with inflation, and any increases in the contract amount. Long run, but intangible factors, such as work force development, and knowledge enhancement are acknowledged, but no attempt is made to assign dollar values to them.

.....the impacts are broadly dispersed with sales increases in all 20 major industry sectors.

[7] Researchers' biographies are contained in Appendix H.

Table 2: Assumptions used for impact assessment	
Fact	**Nebraska**
Population estimates, July 1, 2019, (V2019)	1,934,408
Housing units, July 1, 2019, (V2019)	851,227
Owner-occupied housing unit rate, 2014-2018	66.10%
Median value of owner-occupied housing units, 2014-2018	$147,800
Median selected monthly owner costs -with a mortgage, 2014-2018	$1,352
High school graduate or higher, percent of persons age 25 years+, 2014-2018	91.10%
Bachelor's degree or higher, percent of persons age 25 years+, 2014-2018	31.30%
With a disability, under age 65 years, percent, 2014-2018	7.70%
Persons without health insurance, under age 65 years, percent	9.70%
In civilian labor force, total, percent of population age 16 years+, 2014-2018	69.50%
Median household income (in 2018 dollars), 2014-2018	$59,116
Per capita income in past 12 months (in 2018 dollars), 2014-2018	$31,101
Persons in poverty, percent	11.00%
Total employer establishments, 2017	54,954
Total employment, 2017	833,472
Total annual payroll, 2017 ($1,000)	36,415,429
Population per square mile, 2010	23.8
Land area in square miles, 2010	76,824
FIPS Code	"31"
Source: U.S. Census Bureau	

Area description and assumptions

The next section of this report provides detailed economic impacts of the NG 9-1-1 contract based on the assumptions listed in Table 2. All estimated or projected impacts include direct plus spillover impacts. Table 3 lists year one total impact, or sales impact, from Hamilton's proposed NG 9-1-1 operations for Nebraska. Table 4 contains year one wages and salaries impacts resulting from Hamilton's proposed NG 9-1-1 operations. Table 5 contains year one self-employment income impacts supported by Hamilton's proposed NG 9-1-1 operations. Table 6 contains employment impacts from Hamilton's operations for Nebraska. Table 7 provides state and local tax impacts for Hamilton NG 9-1-1 operations.

Table 3: Total impact by industry of Hamilton's NG 9-1-1	
	Total Year one
Business support services	$5,054,480
Owner-occupied dwellings	$390,420
Food services and drinking places	$237,025
Monetary authorities and depository credit intermediation activities	$201,434
Offices of physicians, dentists, and other health practitioners	$181,990
Private hospitals	$166,775
Non-depository credit intermediation and related activities	$164,168
Wholesale trade businesses	$152,548
Real estate establishments	$151,238
Telecommunications	$143,155
Insurance carriers	$132,997
Securities, commodity contracts, investments, and related activities	$116,497
Employment services	$88,514
Management of companies and enterprises	$74,762
Management, scientific, and technical consulting services	$70,768
US Postal Service	$69,983
Other state and local government enterprises	$69,959
State and local government electric utilities	$69,228
Services to buildings and dwellings	$60,383
Nursing and residential care facilities	$58,792
All other industries	$1,748,421
Total	**$9,403,539**
Source: Goss & Associates based IMPLAN Multipliers, 2020	

Table 4: Wage & salary impact by industry of Hamilton's NG 9-1-1	
Business support services	$2,790,091
Offices of physicians, dentists, and other health practitioners	$95,926
Private hospitals	$77,810
Food services and drinking places	$71,678
Non-depository credit intermediation and related activities	$70,396
Employment services	$61,418
US Postal Service	$59,044
Wholesale trade businesses	$57,362
Management of companies and enterprises	$40,053
Management, scientific, and technical consulting services	$37,494
Computer systems design services	$34,134
Nursing and residential care facilities	$33,528
Insurance carriers	$32,678
Monetary authorities and depository credit intermediation activities	$28,444
Retail Stores - Motor vehicle and parts	$25,261
Retail Stores - General merchandise	$24,251
Legal services	$23,690
Telecommunications	$23,295
Accounting, tax preparation, bookkeeping, and payroll services	$23,102
Couriers and messengers	$22,720
All other industries	$546,081
Total	**$4,178,457**
Source: Goss & Associates based IMPLAN Multipliers, 2020	

Table 5: Self-employment income impacts by industry of Hamilton's NG 9-1-1	
	Total Year one
Business support services	$245,293
Offices of physicians, dentists, and other health practitioners	$19,177
Private hospitals	$9,565
Food services and drinking places	$8,811
Non-depository credit intermediation and related activities	$8,619
Employment services	$8,580
US Postal Service	$7,287
Wholesale trade businesses	$6,564
Management of companies and enterprises	$6,087
Management, scientific, and technical consulting services	$5,983
Computer systems design services	$5,710
Nursing and residential care facilities	$4,585
Insurance carriers	$4,369
Monetary authorities and depository credit intermediation activities	$4,001
Retail Stores - Motor vehicle and parts	$3,254
Retail Stores - General merchandise	$3,048
Legal services	$3,000
Telecommunications	$2,957
Accounting, tax preparation, bookkeeping, and payroll services	$2,861
Couriers and messengers	$2,859
All other industries	$59,132
Total	**$421,743**
Source: Goss & Associates based IMPLAN Multipliers, 2020	

Table 6: Employment impact by industry of Hamilton's NG 9-1-1	
	Total Year one
Business support services	103
Food services and drinking places	5
Employment services	3
Real estate establishments	2
Offices of physicians, dentists, and other health practitioners	2
Private hospitals	1
Non-depository credit intermediation and related activities	1
Services to buildings and dwellings	1
Nursing and residential care facilities	1
Retail Stores - Food and beverage	1
Retail Stores - General merchandise	1
Wholesale trade businesses	1
Securities, commodity contracts, investments, and related activities	1
Civic, social, professional, and similar organizations	1
US Postal Service	1
Retail Nonstores - Direct and electronic sales	1
Couriers and messengers	1
Private household operations	1
Monetary authorities and depository credit intermediation activities	1
Computer systems design services	1
All other industries	18
Total	**146**
Source: Goss & Associates based IMPLAN Multipliers, 2020	

Table 7: State and local tax impacts from Hamilton operations, year one			
	Local	State	Total
Property tax	$99,717	$0	$99,717
Sales tax and gross receipts	$16,514	$80,628	$97,142
Individual income tax	$0	$89,612	$89,612
Corporate income tax	$0	$6,575	$6,575
Other taxes & fees	$43,213	$18,520	$61,733
Total	$159,444	$195,335	**$354,779**
Source: Goss & Associates based IMPLAN Multipliers, 2020			

Appendices: Description of Methodology

Appendix A - Types of Economic Impacts

The economic impacts identified in this study are short-run in nature and represent annual, recurring events. Long run, but intangible factors, such as work force development, and knowledge enhancement are acknowledged, but no attempt is made to assign dollar values to them.

The next section of this report provides detailed economic impacts of the NG 9-1-1 services contract based on the assumptions listed in Table 2. All estimated or projected impacts include direct plus spillover impacts.

Economic impacts can be divided into direct, indirect and induced. The most obvious ***direct impact*** of the NG 9-1-1 services contract on the economy comes in the form of salaries to Hamilton workers residing in the area. ***Indirect impacts*** come from expenditures by Hamilton vendors to their suppliers. Employees of the supplying firms then spend their wages and salaries in the State of Nebraska. This re-spending, or second round multiplying, is referred to as an ***induced*** impact. From an economic perspective, the dollars that remain and are recirculated in the area's economy are very powerful in generating jobs and income for the area.

Direct Economic Impacts. NG 9-1-1 service revenues flowing into the area have direct economic effects on the local economy by making expenditures for goods and services and by paying employee salaries. In addition, expenditures by Hamilton employees from other areas of the country visiting the State of Nebraska produce direct impacts on the region affecting, for example, the area's lodging industry.

Indirect Economic Impacts. The NG 9-1-1 services contract will also produce indirect economic effects on the area economy. For example, hotels and lodging establishments that house Hamilton remote employees and guests who buy merchandise from area wholesalers produce economic impacts.

Furthermore, NG 9-1-1 service expenditures encourage the startup and expansion of other businesses related to the contract. The NG 9-1-1 services contract generates indirect effects by increasing: (a) the number of firms drawn to a community, (b) the volume of deposits in local financial institutions, and (c) economic development.

Induced Economic Impacts. Induced impacts in the region occur as the initial spending feeds back to industries in the region when workers in the area purchase additional output from local firms in a second round of spending. That is, NG 9-1-1 services spending increases overall income and population, which produces another round of increased spending adding to sales, earnings and jobs for the area. NG 9-1-1 services spending is re-circulated creating overall spending that is a multiple of the initial expenditure. This is termed the multiplier effect and is discussed in the next section.

The impacts are broadly dispersed with sales and earnings increases in all 20 major industry sectors.

Appendix B - The Multiplier Effect

When employees of Hamilton spend their salaries within the community, the spending filters through the local economy and causes increased overall spending greater than the initial spending. The impact of this re-spending is known as the multiplier effect. Economic impacts that take place outside the local economy, for example NG 9-1-1 services spending in Kansas City, Missouri, are called leakages and reduce the multiplier and overall impacts. They are excluded when estimating regional economic impacts.

While the direct effects of the NG 9-1-1 services contract can be measured by a straightforward methodology, the indirect and induced effects of NG 9-1-1 services spending must be estimated using regional multipliers.

NG 9-1-1 services spending increases overall income and population, which produces another round of increased spending adding to sales, earnings and jobs for the area.

Community characteristics that affect leakages, and consequently the multiplier, include:

Location. Distance to suppliers affects the willingness to purchase locally. For example, if Nebraska firms are unable to provide supplies to service the contract and there are businesses outside Nebraska that can furnish the needed products and/or services, then vendors will be encouraged to spend outside the area. This results in greater leakages, lower multipliers and smaller impacts.

Population size. A larger population provides more opportunities for companies and workers to purchase locally. Larger population areas are associated with fewer leakages and larger multipliers.

NG 9-1-1 services spending outside the local economy, for example spending in Kansas City, Missouri is called a leakage and reduces the multiplier and overall impacts.

Type of Industry. A community will gain more if the inputs required by local industries for production match local resources and are purchased locally. Thus, over time, as new firms are created to match the requirements of the NG 9-1-1 services contract, leakages will be fewer, resulting in larger multipliers and impacts. For example, wholesale firms in Nebraska will expand to meet the increasing demands of the NG 9-1-1 services contract. Over time, these impacts grow.

While the direct effects of NG 9-1-1 services spending can be measured by a straightforward methodology, the indirect and induced effects must be estimated using regional multipliers.

Appendix C discusses the selection of an estimation technique to measure the direct, indirect and induced impacts of the NG 9-1-1 services contract on Nebraska.

Many types of public and private sector decisions require an evaluation of probable regional effects. Since important impacts are often economic, this requirement has created a need for regional economic impact models. The three most common types of impact models are economic base, econometric, and input-output (I-O). Two of the three impact models have inherent disadvantages that markedly reduce their viability for estimating the impact of NG 9-1-1 services spending on the Nebraska economy.

Appendix C - Choosing a Technique to Measure Impacts

Economic Base Models. Economic base models divide the economy into two sectors -- the local/service sector and the export sector. The economic base multiplier is an average for all the economy making it impossible to distinguish, for example, the impact of the NG 9-1-1 services contract from that of a new manufacturing plant.

Econometric Models. Econometric models use past data to statistically link sectors of the economy. Econometric models have two major weaknesses. First, the time series data used in constructing econometric models are often unavailable at the county and metropolitan area level, thus precluding county-level analysis. This is especially true for rural counties and for counties with small populations. Second, econometric models are costly to build and maintain.

Input-Output (I-O) Models. I-O models are the most frequently used types of analysis tools for economic impact assessment. Input-output is a simple general equilibrium approach based on an accounting system of injections and leakages. Input-Output analysis assumes that each sector purchases supplies from other sectors and then sells its output to other sectors and/or final consumers.

Historically, high costs precluded the extensive use of I-O models in regional impact analysis. However, with the advent of "ready-made" multipliers produced by third parties, such as the U.S. Forestry Service, I-O multipliers became a much more viable option for performing impact analysis.

All purely non-survey techniques or "ready-made" multipliers take a national I-O table as a first approximation of regional inter-industry relationships. The national table is then made region-specific by removing those input requirements that are not produced in the region.

I-O models are the most frequently used analysis tools for economic impact assessment.

Input-Output systems were originally developed by Wassily Leontief (1941) to assist in planning a national economy. Input-Output represents an effective method for depicting and investigating the underlying processes that bind industries of a region. It provides a technique to project into the future the magnitude of important additions or injections into the local economy.

Appendix D - Input-Output Models
A Preferred Methodology

Input-Output models are composed of three basic tables. The first, the Transactions Table, traces inter-industry sales and purchases within a defined region. The next table, the Direct Requirements Table, answers the question, "If a certain dollar value of intermediate requirements is present for a total dollar value of gross output, what are the intermediate requirements for each industry per dollar of gross output?" The manipulation of these two tables result in the final and most important of the tables, the Industrial Multiplier Table. This table is then used to calculate overall impacts.

Chief problems involved in the use of multipliers are:

Selection of Industries. For which industries will impacts be estimated? The selection is generally dictated by definitions used by government agencies that collect the data. For example, most government data do not distinguish employment in a cardiac center or clinic from that in a hospital.

Selection of a Region. Again, government agencies collect aggregate data by county, thus requiring the analysis to take place at the county level, or combination of counties. Most developers of "ready-made" multipliers use the County Business Patterns as the primary data source. For this study, the State of Nebraska is the area of analysis.

For this study, the State of Nebraska is the area of analysis.

Major assumptions of the I-O model

- **Constant production coefficients**. For example, it is assumed that "x" dollars of new revenues flowing to the State of Nebraska will produce "y" dollars of output regardless of the scale of operations. In other words, the I-O model assumes constant returns to scale.
- **Constant technological relationships between inputs and outputs**. Thus, I-O multipliers assume that technology remains the same between the time the multipliers are calculated and the period for which impacts are estimated.
- **Old purchasing patterns are the same as new purchasing patterns**. Thus, it is assumed that purchasing patterns between Hamilton and its suppliers in the State of Nebraska will be the same as other firms in the industry in the area.
- **No supply constraints**. I-O models do not take into consideration the problem of finding an adequate supply of workers to fill new jobs brought about by the NG 9-1-1 services contract.[8]

[8]Bartik (1991) estimated that 75% of the net new jobs resulting from a business expansion or business relocation go to in-migrants.

Appendix E - IMPLAN Multipliers Used in this Study

The Forestry Service of the U.S. Department of Agriculture developed the IMPLAN multi- pliers in the 1980s (U.S. Forest Service, 1985). For very populous areas, IMPLAN divides the economy into 528 industrial sectors. Industries that do not exist in the region are automatically eliminated during user construction of the model (e.g. coal mining in Hamilton County). IMPLAN uses an industry-based methodology to derive its input-output coefficients and multipliers. Primary sources for data are County Business Patterns data and Bureau of Economic Analysis data.

IMPLAN and RIMS (Regional Input-Output Modeling System) are two of the most widely used multiplier models. IMPLAN has been compared to other multiplier systems and found to produce reliable estimates (Hughes, et al., 1991; Rickman and Schwer, 1993). Likewise, Crihfield and Campbell (1991), in estimating the impacts of opening an automobile assembly plant, concluded that IMPLAN's outcomes are, on balance, somewhat more accurate than RIMS.

IMPLAN multipliers possess the following advantages over other I-O Multiplier Systems:

- Price changes are accounted for in the creation of the multipliers.
- Employment increases or decreases are assumed to produce immediate in- or out-migration.
- Multipliers are produced at reasonable costs by third party vendors.

This study uses the IMPLAN multipliers.

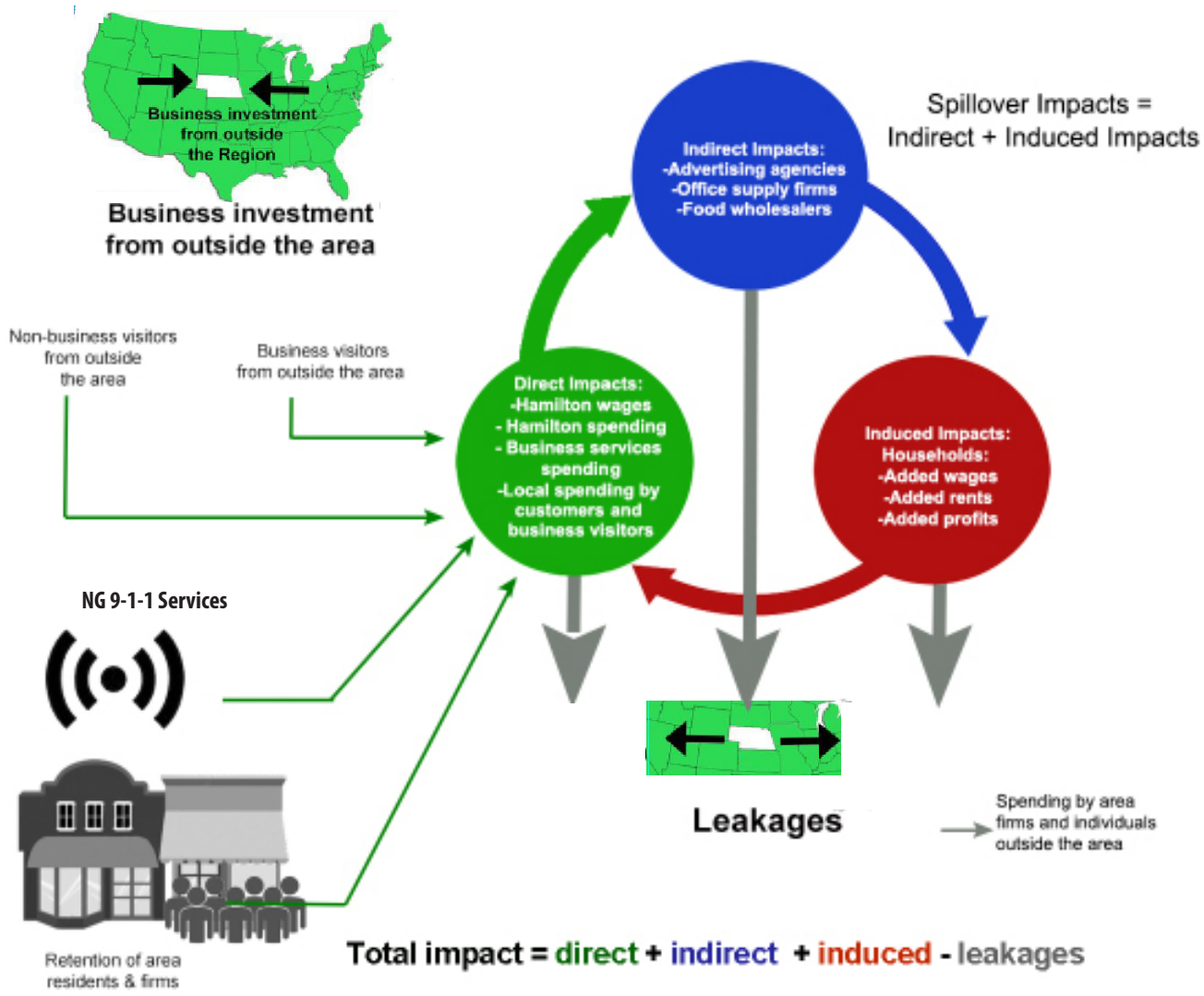
Table 8: Multipliers provided by IMPLAN and used in this study

Type of Multiplier	Description
Output Multipliers	Total industry output per $1 change in final demand
Labor Income Multipliers	Total household earnings per $1 change in final demand
Employment Multipliers	Total number of jobs per $1 million change in final demand

Source: Goss & Associates 2017

Appendix F - Schematic of Sample NG 9-1-1 Services Impacts

Figure F.1: Schematic of Sample NG 9-1-1 Services



Source: Goss & Associates, 2020

Appendix G - References

Bartik, T. Who benefits from state and local economic development policies? Kalamazoo, MI: W.E. Upjohn Institute, 1991.

Christianson, J. and L. Faulkner. "The Contribution of Rural Hospitals to Local Economies." Inquiry, Vol. 18(1), 1981, pp. 46-60.

Crihfield, J. B. and Harrison S. Campbell. "Evaluating Alternative Regional Planning Models." Growth and Change, 22, 1991, pp. 1-16.

Erickson, R. A. Gavin, N. and S. Cordes. "The Economic Impacts of the Hospital Sector." Growth and Change, Vol. 17, pp. 17-27.

Farmer, F.L., M.K. Miller and D.E. Voth. "Evaluation of Rural Health Care Programs Employing Unobserved Variable Models: Impact on Infant Mortality." Rural Sociology, Vol. 95(1), 1991, pp. 127-142.

Garrison, Charles. "The Impact of a Rural Hospital on Economic Development." Growth and Change, 1974.

Gooding, E.P. and S.J. Weiss. "Estimation of Differential Employment Multiplier in a Small Regional Economy." Research Report No. 37, 1966, Federal Research Bank of Boston, Boston, MA.

Goss, E.P. and G.S. Vozikis. "High Tech Manufacturing: Firm Size, Industry and Population Density." Small Business Economics, Vol. 6(3), 1994, pp. 291-297.

Hoffman, M., J.J. Jimason and W.C. McGinly. "The State of U.S. Hospitals in the Next Decade: A Review of the Hospital Crisis." National Association for Hospital Development, 1989, Falls Church, VA.

Hughes, D., Holland, D. and P. Wandschneider, "The Impact of Changes in Military Expenditures on the Washington State Economy." The Review of Regional Studies, Vol. 21(3), 1991, pp. 221-234.

Krahower, J. Y., Paul Jolly and Robert Beran. "U.S. Medical School Finances." Journal of the American Medical Association, September 1, 1993, Vol. 270(9), pp. 1085-1092.

Leontief, W. The Structure of the American Economy, 1919-1929. New York: Oxford University Press, 1941.

Leslie, L. and P.T. Brinkman. The Economic Value of Higher Education. MacMillan Publishing Company, New York. 1988.

Lewin/ICF, Division of Health and Sciences and Research, Inc. 1988. Critical Care in Jeopardy, Washington, D.C.

McDermott, R.E., G.C. Cornia and R.J. Parsons. "The Economic Impact of Hospitals in Rural Communities." Rural Health Policy, Vol. 7(2), 1991, pp. 117-133.

McHone, Warren. "Practical issues in measuring the impact of a cultural tourists event in a major tourist destination." Journal of Travel Research, Vol. 38(3), pp. 299-302.

Milward, B. H. & Newman, H. H. (1989). State incentive packages and the industrial location decision. Economic Development Quarterly, 3(3), 203-222.

Moore, C. "The Impact of Public Institutions on Regional Income: Upstate Medical Center." Economic Geography, Vol. 50, 1974, pp. 124-129.

Naughton, John and J.E. Vana. "The Academic Health Center and the Healthy Community." American Journal of Public Health, July 1994, Vol. 94 (7), pp. 1071-1076.

Rickman, D.S. and R. K. Schwer. "A Systematic Comparison of the REMI and IMPLAN Models: The Case of Southern Nevada." Review of Regional Studies, Vol. 23 (2), 1993, pp. 143-161.

U.S. Forestry Service. 1991 IMPLAN Multiplier Reports, Minnesota IMPLAN Group, Inc., 1995, Stillwater, MN.

Appendix H - Researchers' Biographies

Ernie Goss is the Jack MacAllister Chair in Regional Economics at Creighton University and is the initial director for Creighton's Institute for Economic Inquiry. He is also principal of the Goss Institute in Denver, Colo. Goss received his Ph.D. in economics from The University of Tennessee in 1983 and is a former faculty research fellow at NASA's Marshall Space Flight Center. He was a visiting scholar with the Congressional Budget Office for 2003-2004, and has testified before the U.S. Congress, the Kansas Legislature, and the Nebraska Legislature. In the fall of 2005, the Nebraska Attorney General appointed Goss to head a task force examining gasoline pricing in the state.

He has published more than 100 research studies focusing primarily on economic forecasting and on the statistical analysis of business and economic data. His book Changing Attitudes Toward Economic Reform During the Yeltsin Era was published by Praeger Press in 2003, and his book Governing Fortune: Casino Gambling in America was published by the University of Michigan Press in March 2007.

He is editor of Economic Trends, an economics newsletter published monthly with more than 11,000 subscribers, produces a monthly business conditions index for the nine-state Mid-American region, and conducts a survey of bank CEOs in 10 U.S. states. Survey and index results are cited each month in approximately 100 newspapers; citations have included the New York Times, Wall Street Journal, Investors Business Daily, The Christian Science Monitor, Chicago Sun Times, and other national and regional newspapers and magazines. Each month 75-100 radio stations carry his Regional Economic Report.

Scott Strain is a senior research economist at Goss & Associates. He has worked as an economist and statistician for more than 20 years providing forecasts and analysis across a wide-range of industries. Scott served as an industry economist, working in new product development regarding both quantitative and qualitative research. Strain was Senior Director of Research for an economic development agency, providing economic impact and tax incentive analysis to both private businesses and government entities. He served on the business advisory committee that worked with Nebraska state senators and the director of the state's Economic Development Department to develop the Nebraska Advantage Act – a comprehensive package of business incentives that has helped to add more than $6 billion in new capital investment and over 13,000 new jobs in the State of Nebraska since the Act's inception in 2006.

HAMILTON APPENDIX 4: HAMILTON FINANCIAL OVERVIEW

(CONFIDENTIAL & PROPRIETARY INFORMATION)

Page intentionally left blank.

To view Hamilton Financial Overview, please see, "**PROPRIETARY INFORMATION**" electronic file.

HAMILTON APPENDIX 5: HAMILTON RESUMES AND REFERENCES

Peggy Christensen

1006 12th Street, Aurora, NE, 68818 · (402) 694-5101 · peggy.christensen@hamiltontel.com

PROFESSIONAL PROFILE

Experienced leader in the telecommunications and financial services industries. Skilled expertise in the following degrees of focus:

- Leading change
- Business transformation
- Project management
- Software development methodologies and implementation
- Business process improvement
- Team building

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, NE

Manager of Enterprise Software & Data Services, 2016 – Present

- Lead a varied group of enterprise software, data and project management software professionals.
- Lead services model.
- Improve communication and business process.
- Team development.

Hamilton Telecommunications – Aurora, NE

Project Manager, 2015 – 2016

- Lead teams to deliver projects and new products.
- Implementation of software development methodology and programs.
- Leading programs for ongoing enterprise software governance.

Suntrust Bank – Atlanta, GA

Demand Manager, Consumer Business Information Office (CBIO), 2014 – 2015

- Led demand and capacity management.
- Championed and led process improvement initiatives.
- Acted as the liaison between CBIO and internal clients in the line of business; ensured effective communication.
- Drove implementation of new demand management software.

Suntrust Banks – Atlanta, GA

Portfolio Manager, Consumer Portfoliio Program Management Office, 2010 – 2014

- Led a team of Program and Project Managers leading initiatives across multiple areas of the Consumer Bank – including Retail, Risk, Data & Analytics and Card Products.
- Built relationships across the bank (e.g. business, technology, risk, Anti-Money Laundering/Bank Secrecy Act, strategic sourcing, legal, compliance) in order to deliver new products and functionality to bank clients.
- Ensured alignment among executives and program sponsors and stakeholders.
- Managed relationships with vendor personnel for delivery of product solutions.

- Developed strategies and business cases; drove program/product delivery in order to deliver benefits.
- Ensured projects and programs adhere to the prescribed project management and software development life cycle (SDLC) methodologies.
- Developed 3-year product planning roadmaps in conjunction with product management and technology organizations.

FIS (Formerly Metavante) – Dallas, TX
Application Development Program Manager, 2006 – 2010

- Managed a program consisting of multiple software development projects.
- Determined development capacity against demand for adding new functionality into several applications.
- Managed the risks, issues and financial concerns (including offshore contracts) of the software development program.
- Managed a team of project managers, business analysts and technical writers.
- Acted as escalation point for projects assigned to project managers on my team.
- Ensured projects and programs adhered to the prescribed software development life cycle (SDLC) methodology (completing a migration from waterfall-style practices to agile).
- Developed new and improve existing processes and procedures amongst development, support and implementation teams.

Alogent Corporation – Alpharetta, GA
Professional Services Manager, 2004 – 2006

- Managed a team of Professional Services personnel.
- Acted as escalation point for projects assigned to Implementation Managers on my team.
- Developed and documented project/professional services engagement estimates.
- Wrote Statements of Work for client engagements.
- Acted as an Implementation Manager and/or Senior Business Analyst.
- Provided customer service and satisfaction on assigned engagements.
- Assisted business development and sales personnel on sales calls with potential clients.
- Coordinated sales proposals and RFI/RFP responses for Professional Services Team.
- Developed new and improved existing Professional Services processes and procedures.
- Developed and maintained process and design document templates for company use.

Alogent Corporation – Alpharetta, GA
Senior Business Analyst, 2001 – 2004

- Managed all aspects of software implementation projects in the US and abroad.
- Developed and maintained project plans for assigned projects.
- Wrote design documents and platform specifications for software implementation projects.
- Developed business rules and configured software for client implementations.
- Trained client personnel on software business rules and configuration management.
- Liaised with development and quality assurance teams during project lifecycle.
- Developed client-training materials and delivered classes to clients and internal staff.

Paysys International – Norcross, GA
Senior Business Analyst, 2001 – 2004

- Assisted with development of object oriented, web-enabled software for the business-to-business (B2B) marketplace.

- Acted in a business development role for potential clients of new applications.
- Served as lead business analyst and project manager for B2B application development project.
- Developed mentoring program for new-hire business analysts.
- Assisted with development of commercial card application in object oriented, web-enabled, client server environment.
- Experienced with XML data formats.

Equifax Card Solutions – Atlanta, GA

Business Analyst / Senior Business Analyst, 1996 - 2000

- Experience with full life-cycle software development projects in the US and abroad.
- Ability to gather customer requirements, perform gap analyses and translated into functional solution documents for software application development or change.
- Project management experience using MS Project.
- Data conversion experience in a mainframe environment, including data mapping for complex financial systems, the verification and testing of thousands of converted records, and post-conversion troubleshooting and support.
- Experience developing test plans, test cases, writing and execution of test scripts, and tracking and resolution of variances using an MS Access database and reports.
- Experience implementing new software in a mainframe.
- Experience with flexible, table-driven software in a large, complex processing environment. This included up-front planning and set-up through production management.
- Managed team of project-oriented conversion analysts (7 direct reports).

EDUCATION

Bellevue University – Bellevue, NE
Certifications in Operational Leadership & Professional Banking

University of Nebraska – Lincoln, NE
Bachelors Degrees in Business, English, & Consumer Science Education

CERTIFICATIONS & KEY ACCOMPLISHMENTS

- Project Management Certification (PMP) - 2004
- Pragmatic Marketing Certifications I, II & III – 2016
- Newcomer Award, Quest International Users Group – 2018
- Change Management Practitioner, Prosci – 2018

REFERENCES

Lisa Klingberg,
Co-Founder & Managing Partner, Inver Consulting

Tom McDermott
Co-Founder & Managing Partner, Inver Consulting

Douglas McCarthy
Vice President Sales & Business Development, iLearnERP

James M. Ediger

1006 12th Street, Aurora, NE, 68818 · (402) 694-9358 · jim.ediger@hamiltontel.com

PROFESSIONAL PROFILE

Legal advisor with extensive experience in statewide utility and public safety collaboration. As representative of Hamilton Telecommunications, Ediger serves at the forefront of negotiation, compliance regulation and operational infrastructure.

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, NE

General Counsel, 2015 – Present

- Serve as in-house general counsel for seven diverse business entities that encompass Nedelco, Inc., d/b/a Hamilton Telecommunications, with offices in seven states
- Advise on complex regulatory and compliance matters; review, draft and negotiate contracts and manage insurance matters for all entities
- Work directly with senior management and the board of directors to resolve legal matters

Kelley, Scritsmier & Byrne, P.C., L.L.O. – North Platte, NE

Associate Attorney, 2013 - 2015

- Advise business clients with a wide range of matters, including entity formation, contracts, tax matters, shareholder agreements and liquidation and dissolution
- Draft real estate documents, including purchase agreements, lease agreements, promissory notes, deeds of trusts, section 1031 exchange agreements, deeds, easements and covenants
- Work with estate planning clients to create customized estate plans tailored for their individual needs, which included the preparation of wills, trusts, health care directives and powers of attorney

ADMISSIONS

Nebraska Sate Bar, 2013

- State Bar No. 25232

United States District Court, 2013

- District of Nebraska

CERTIFICATIONS

Nebraska State Bar Association (Member); Nebraska State Chamber (Hamilton Representative); Nebraska Rural Independent Companies (Hamilton Representative on steering and science committees); Nebraska Telephone Association (Hamilton Representative); Nebraska Advocacy Group (Hamilton Representative); National Emergency Number Association (Member); NTCA, Rural Broadband Association (Hamilton Representative); Nebraska NG911 Working Group (Member)

EDUCATION

University of Nebraska College of Law – Lincoln, NE
Juris Doctor (J.D.), 2010 – 2013

- Business Program of Concentrated Study
- Entrepreneurship Clinic
- Law Clerk at Jacobsen, Orr, Lindstrom, & Holbrook, P.C., L.L.O. – Kearney, NE

University of Nebraska-Lincoln – Lincoln, NE
Bachelor of Science in Business Administration, 2006 – 2009

- Major: Accounting; Minor: Economics
- Study Abroad Program: Oxford University – Oxford, England
- Alpha Tau Omega Fraternity (Treasurer)

REFERENCES

David O'Connor
Attorney, Wilkinson, Barker, Knauer LLP

Dan Caldwell
President, Consortia Consulting

Bryan Slone

Wayne Hahn

1001 12th Street, Aurora, NE, 68818 · (402) 694-5101 · wayne.hahn@hamiltontel.com

PROFESSIONAL PROFILE

Over 30 years of IT experience specializing in insuring Wide Area Network (WAN) related technological solutions are engineered, configured, and maintained in a manner that allows systems to operate at optimal levels of reliability and functionality. Professional strengths include:

- Maintaining and further developing a highly functional team to deliver superior, predictable, and reliable services.
- Establishing and maintaining the right staff, processes, and technologies to meet all business objectives and expectations.
- Provides leadership role for making WAN decisions, interfacing with key stakeholders, and prioritizing individual and team work efforts
- Analyzing and creatively problem solving, assessing all potential risks and advantages.

PROFESSIONAL EXPERIENCE

HAMILTON TELECOMMUNICATIONS, Aurora, NE

WAN Manager and Network Engineer, August 1988 – Present

- Acts as a working manager to ensure network systems are operating sufficiently to deliver quality services.
- Reviews problem tickets and other reports/tools to identify risks to network system availability; follows and enhances the processes that measure, monitor, and report on the availability and performance of all network systems.
- Participates in project implementations.
- Supervises work of WAN staff involved in network activities, including maintenance of firewall, switches, and routers, and all outsourced network projects.
- Develops standards and procedures to ensure quality assurance; reviews change control processes and regulatory adherence.
- Provides input on architecture of projects involving technology and connectivity between sites, customers, and vendors.
- Develops documentation of network controls and functionality, as well as policies, procedures, and standards for best practices; responsible for implementation.
- Analysis of new technologies and recommendations for future enhancements.
- Maintains network and data security, including knowledge of latest technologies and threats.
- Provides support and troubleshooting for networks, Linux, and UNIX servers.
- Prepares documentation of technical information, recovery, and maintenance procedures.
- Resolves system outages and provides timely reports and final disposition.
- Maintains excellent relationships with all management, employees, and customers.

EDUCATION

CENTRAL COMMUNITY COLLEGE, Hastings, NE

Associates of Applies Sicence in Computers and Automation, 1988
Associates of Applied Sicence in Digital Electronics, 1988

ADDITIONAL SKILLS

Extensive experience in computer system networking, switch management, software development and maintenance and telecommunications technology management.

- UNIX System Administration
- UNIX Shell Programming
- T1 Installation and Troubleshooting
- C Programming
- TCP/IP Networking
- PC Troubleshooting
- X25 Networking

REFERENCES

Dustin Curtis
IP Network Specialist, RVW, Inc.

Adam Self
Support Engineer, Midax

Daren Chrisinger
Vice President, Cozad Telephone Company

Jeffery Knighton

1006 12th Street, Aurora, NE, 68818 · (402) 694-5101 · jeff.knighton@hamilton-innovations.com

PROFESSIONAL PROFILE

Over twenty years of experience in designing, developing and deploying telecommunication products and services that serve the Deaf and Hard of Hearing community. Professional strengths include:

- New software development.
- Innovative research.
- Extensive experience in communication based technology.

PROFESSIONAL EXPERIENCE

Hamilton Innovations – Tucson, AZ

President, 2015 – Present

- Responsible for managing new products and software development.
- Research and technical assistance for NG 9-1-1 and Traditional Relay Service technology.
- Innovation of first web-browser to TTY communication system, and "IP Relay".
- Designed and developed software for low-vision users to effectively use telephones.
- Developed a TTY algorithm that has been widely used in various industries, including telecommunication relay services, public safety and business communication environments.
- Managed the launch of Hamilton CapTel for Business Interconnected by Tenacity.

Voiceriver, Inc. – Tucson, AZ

President / Founder, 2004 - 2015

- Perform all aspects of running a successful company, including writing proposals, interacting directly with customers, managing finances, and developing company processes and procedures.
- Design and manage the development of call-center platform components for the Telecommunication Relay Industry (TRS).
- Develop and deploy niche-based communication solutions for TRS, Emergency 911 and Prison/Correctional facilities industries currently processing millions of production call interactions each month.
- Developed software modem algorithms for Baudot, Turbocode and ETurbo text.
- Incorporated Agile-based software development processes within the company based on Scrum methodology.
- Oversee and develop mobile, web, desktop, embedded, database, and server based software using a variety of programming languages and frameworks including:
    - Mobile: Android (Java) and IOS (Objective C)
    - Desktop (Windows): C#, Visual C++, Visual Basic
    - Web: Html, CSS, JQuery, Web Sockets, PHP, ASP, Cold Fusion
    - Embedded: C, C++, ASM (Texas Instruments & Analog Devices)
    - Database: MS SQL Server, mysql
    - Server: C, C++, Java (Linux and Windows-based systems)

NOTABLE VOICERIVER CLIENTS + PROJECTS

Callpointe.com, 2005 – 2015

Callpointe provides an automated medical patient notification service via telephone calls, emails and text messages to inform patients about upcoming medical appointments. I was the primary software engineer on the telephony platform that actually places the automated calls, detects when a person or answering machine has answered the call, and subsequently delivers a recorded message customized to the individual's upcoming medical appointment.

Hamilton Relay, 2011 – Present

Voiceriver designed and developed a telephony appliance for Hamilton, for use in their traditional TRS call center environment. It was designed to comply with both state and federal requirements for TRS, including having modem functionality that would allow Hamilton Communication Assistants to communicate with TTY and other text capable devices over a standard telephone line. My role was to oversee the project from Voiceriver's side, which included creating design documents and project schedules, as well as work with other engineers, both on the Voiceriver side and on the Hamilton side to implement the required functionality and integrated the appliance into Hamilton's production environment. I was also the primary software developer on all of the modem algorithms needed for state and federal compliance. The primary project was completed around the summer of 2012. Following the completion, I continue to be involved intermittently for various support issues that occasionally arise surrounding the appliance.

Tenacity Inc., 2009 – Present

Tenacity designs, develops and sells telephony software to provide accessibility support to people with lowvision, mobility impairment, and hearing impairment to communicate effectively over a telephone. In 2009, Tenacity brought to market a software application "ipTTY," which Voiceriver had been developing since 2005. It is a VoIP softphone application that can be used with any VoIPbased phone system to allow a user to use their computer to communicate directly with remote party that has a TTY machine. Tenacity has contracted all of their software development services and ongoing software support services to be provided by Voiceriver, and I oversee these services, and often perform some of the ongoing improvements to Tenacity's suite of software programs. As part of my technical involvement with ipTTY, I was able to participate in presentation to the US Access Board, and to FCC officials regarding technology designed to improve telecommunications for the deaf with respect to VoiceoverIP systems. Other participants in this presentation included representatives from the Trace Center at the University of Wisconsin, Gallaudet University, and Omnitor SE.

Sprint – Overland Park, KS

Telephony Engineer / Consultant, 2004 – 2005

- Developed a prototype call center platform for performing TRS (Telecommunication Relay Services). This involved a mixture of call setup/tear down protocols (CAS, Q.931,SS7), voice protocols (G.711, PCM) as well as text protocols (v.34, v.32, v.32bis, v.22, v.22bis, Bell 103, v.21, Baudot, Turbocode, Eturbo).
- Incorporated and used signal processing capabilities including echo cancellation, audio stream conferencing, FSK modulation/demodulation, DTMF detection, and speech detection.
- Developed client application for an agent to perform TRS

Nxi Communications, Inc. – Salt Lake City, UT
Chief Technical Officer / Senior Software Engineer, 1997 – 2004

- Designed and developed Nxi's softswitch telephony platform known as the "NTS" system. This included protocols for call setup/teardown(Q.931, SIP, Nxi Proprietary), media streams: (RTP/RTCP, G.711, Speex, iLBC), and text communications (modem protocols).
- Developed concepts behind web browser to TTY communications, including developing the initial client implementation (java applet) of the client-server implementation used by both MCI and Sprint. Also designed the protocol between the client-server implementation.
- Designed and programmed a "Nextalk.net", web service used by deaf users to place text telephone calls using the Internet.
- Designed and developed a call center platform for Sprint Relay for their traditional TRS service based on NXi technology.
- Received patents: #6501779, 7555521

EDUCATION

Brigham Young University – Provo, UT
Bachelors of Science in Electrical Engineering, 1996
Minor: Mathematics
Emphasis: Computer Systems and Digital Design

REFERENCES

Christy Williams
Director, North Central Texas Emergency Communications District

Tommy Tran
9-1-1 Solutions Architect, North Central Texas Emergency Communications District

Richard Ray
ADA Technology Access Coordinator, City of LA Dept. on Disability

Robert G. Leonard

1001 12th Street, Aurora, NE, 68818 · (402) 694-5101 · robert.leonard@hamiltontel.com

PROFESSIONAL PROFILE

Over 20 years of IT experience specializing in Cyber Security, Active Directory Management, implementation of enterprise software solutions and end user support. Specializing in working with federal government agencies to help guide efforts to reach a uniform and all-encompassing cyber security standard. Professional strengths include:

- Active Directory
- SQL Server
- Application Troubleshooting
- Program Management
- Cyber Security
- Backup/Recovery Implementation
- LAN Administration
- Corporate Anti-Virus Implementation
- Network Shares and Security
- Outstanding Customer Service Skills

PROFESSIONAL EXPERIENCE

HAMILTON TELECOMMUNICATIONS, Aurora, NE
Security Manager/LAN Administrator, 2003 – Present

- Management of Active Directory network with 800 users in over seven states
- Implementation of 12 corporate-wide software solutions
- Cyber Security Expert
- Implemented mobile data for network shares to phones, tablets and other mobile devices
- Implementation of backup solution for servers and endpoints
- VPN administration
- Implementation and management of encryption software for PCI compliance

ABACUS BUSINESS SYSTEMS, INC., Grand Island, NE
General Manager, 2000 - 2003

- Responsible for 11 employees and overall business management
- Implemented first wireless mobile data for law enforcement in Nebraska
- Managed over 200 users in multiple sites for county government network

UNITED STATES ARMY
Specialist, 2005 - 2013

- Served over eight years in the United States Army as a Cavalry Scout and in combat operations in Afghanistan during Operation Enduring Freedom
- Trained machine gunner and combat lifesaver
- Expert in combat operations, counter-intelligence, and counter-insurgency

EDUCATION

CENTRAL COMMUNITY COLLEGE, Columbus, NE
Associates of Applied Science in Information Technology, 2001
Diploma in both Electronics and PC Repair

REFERENCES

Michael R. Overly, Esq., CISA, CISSP, COP, CIPP, ISSMP, CRISC
Partner, Information Technology and Outsourcing Group, Foley & Lardner LLP

Jesse Ward
Director & Policy Analysis, NTCA

Patrick Williams
Client Manager, Optiv Security, Inc.

Seth Marks

1006 12th Street, Aurora, NE, 68818 · (402) 694-5101 · seth.marks@hamilton-innovations.com

PROFESSIONAL PROFILE

Over sixteen years of progressive experience as a product development leader. Capable of organizing cross-functional teams to efficiently analyze and solve large-scale problems with cost effective solutions. Professional strengths include:

- New software development.
- Innovative troubleshooting, problem solving and collaboration.
- Extensive experience in communication based technology.

PROFESSIONAL EXPERIENCE

Hamilton Innovations – Tucson, AZ

Vice President of Engineering, 2015 – Present

Raytheon – Tucson, AZ

Sr. Principal Software Engineer – Raytheon Missile Systems, 2009 – 2015

- Integrated Program Team Lead for the Standard Missile 3 software team. Leader of cross functional teams of 30-50 engineers.
- Responsible for delivery of 10 – 30 million dollar budgets with aggressive schedules and complex dependencies.
- Section Manager responsible for personnel management including performance development and hiring/team building for the Standard Missile 3 software teams.
- Manage customer interfaces and software/hardware requirements in support of Critical Design and Non Advocate Reviews.
- Mentor and train front line team leadership including setting expectations/vision.
- Co-Lead for the Raytheon Software Council corporate wide Application Lifecycle Management (ALM) initiative. Worked with Raytheon business units to train and deploy ALM tools.
- Software Team Lead for DARPA Precision Close Air Support proposal resulting in a proposal win. Lead software architecture and design across the team including external Aerospace Partners. Participated in Cursor on Target interface (CoT) definition with the CoT working group.
- David's Sling Weapon System (DSWS) Software REA for the IPG video processor assembly.
- DSWS Team Lead responsible for program level software deliveries. Acting Software Change Control Board Chair.

Motorola – Schaumburg, IL

Principle Staff Software Engineer / Systems Engineer, 2000 – 2009

- Defined product roadmaps for Motorola WiMAX access point including cost analysis to ensure Motorola's ability to produce a competitive product within the budget and time constraints allotted.
- WiMAX architect responsible for creation of Access Point software requirements and architecture to be implemented by 50 software engineers.
- Defined WiMAX Access Point mobility systems solution with technical expertise in Mobile IP, Proxy Mobile IP and Mobility Management.

- IP infrastructure and protocol expert with extensive experience in IPv4, Mobile IPv4, IPv6 and Mobile IPv6 and L2 transport architectures. Defined internal messaging protocols used for system component communications.
- Key architect responsible for defining Quality of Service and Service Flow Management solutions for the WiMAX access point.
- Architecture analysis and design using UML including use case analysis and message sequence design.
- Platform expertise including network processor architecture and hardware specific performance analysis.
- Direct software feature teams to successful on time completion according to aggressive market defined schedules.
- Work with local and remote teams in Russia, China, and India, as well as 3rd party vendors, to produce cohesive cost effective software solutions.
- Act as a mentor to software lead engineers to ensure successful delivery of software solutions through the complete product lifecycle.
- Spearhead the creation and improvement of software processes in order to manage and control complex parallel software development activities to reduce time to market while maintaining quality.
- Contribute to a strong intellectual property and patent portfolio for Motorola in WiMAX technologies.

Vantage Controls – Orem, UT

Electrical and Software Engineer, 1997 – 2000

- Lead hardware and software design of the DMX 512 lighting controller product for use with the Vantage Q home automation system.
- Designed and implemented hardware test solutions to ensure product quality and decrease total cost of product validation through automation of test and validation procedures.
- Developed business analysis tools to organize product and part inventories.
- Technical expertise in embedded C/C++ software development, hardware analysis and design and embedded small systems communication.

Private Consulting – Crystal Lake, IL

Electrical Software Engineer, 1999 – 2013

- Consultant to Voiceriver for development of specialized telecommunication equipment for use by the deaf and hearing impaired.
- Worked with the Blendtec® business team to create requirements and produce control software for their industrial programmable blenders.
- Developed software solution for eFilecabinet® accounting software management tools.

EDUCATION

Illinois Institute of Technology – Chicago, IL
Master of Science in Computer Science

Brigham Young University – Provo, UT
Bachelors of Science in Electrical Engineering

KEY ACCOMPLISHMENTS

- Member of the Software Center Integrated Product Development System Team
- Received the Raytheon Excellence in Leadership Award for 2013
- Graduate of Raytheon Missile Systems Leadership Development Program
- Software Change Control Board Chairman
- Certified Raytheon Teacher for SCRUM and Agile process execution for high performing teams
- Chairman of the WiMAX Access Point Technology Forum
- Member of Motorola Networks Patent Committee
- Member of WiMax System Engineering Change Control Board

REFERENCES

Christy Williams
Director, North Central Texas Emergency Communications District

Tommy Tran
9-1-1 Solutions Architect, North Central Texas Emergency Communications District

Richard Ray
ADA Technology Access Coordinator, City of LA Dept. on Disability

Daniel C. Molliconi

1006 12th Street, Aurora, NE, 68818 · (402) 694-0125 · dan.molliconi@hamiltontel.com

PROFESSIONAL PROFILE

25 years of management and corporate leadership experience at the forefront of the telecommunications and technology industries. A dynamic leader of people, practice and workplace culture.

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, NE
Chief Operating Officer, Nedelco Inc., 2019 - Present

- President, Hamilton Telephone Company
- Vice President, Hamilton.net, Hamilton Information Systems, Hamilton Long Distance, Hamilton NG911
- LAN/WAN Manager

Hamilton Telecommunications – Aurora, NE
Chief Operating Officer of Telecom and Technology, 2017 - 2019

- President, Hamilton Telephone Company
- Vice President, Hamilton.net, Hamilton Information Systems, Hamilton Long Distance
- LAN/WAN Manager

Hamilton Telecommunications – Aurora, NE
Vice President, 2012 - 2017

- VP of Hamilton.net, Hamilton Information Systems, Hamilton Long Distance, Hamilton Telephone Company

Hamilton Telecommunications – Aurora, NE
Vice President, 2007 - 2012

- VP of Hamilton.net, Hamilton Information Systems
- LAN/WAN Manager

Hamilton Telecommunications – Aurora, NE
Vice President, 2001 - 2007

- VP of Hamilton.net
- Corporate Human Resource Manager

Hamilton Telecommunications – Aurora, NE
Corporate Human Resource Manager 1995 - 2001

- Managing human resources for corporate office.

EDUCATION

Hastings College – Hastings, NE
B.A. – Economics, Business Administration and Human Resource Management, 1990

REFERENCES

Kirk Penner
Owner, Penner Manufacturing

Matt Friesen
General Manager, Mainstay Communications

Chris Decker
COO, Aurora Cooperative

John A. Nelson

1006 12th Street, Aurora, NE, 68818 · (402) 694-5101 · john.nelson@hamiltontel.com

PROFESSIONAL PROFILE

CEO of Hamilton Telecommunications and the company's eight business line divisions. As a Director of Nedelco and several of its wholly owned subsidiaries, John provides oversight and leadership to all members of the Hamilton management team and staff.

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, Nebraska

Officer and member of Hamilton Senior Management Team, 2002 - Present
President and CEO of Nedelco, 2015 – Present
Currently: President of Hamilton NG911, Inc., Hamilton Long Distance Company, Hamilton Relay, Inc., Hamilton.net, Hamilton Information Services. Executive Vice President of Hamilton Telephone Company. Vice President of Nedelco Services Corporation.

- Responsible for the strategic direction and management of the Company.
- Provides direction and leadership to members of Hamilton Telecommunications management
- Responsible for Customer, Employee, and Shareholder success.
- Oversees and directs strategic planning and management.

Hamilton Telecommunications – Baton Rouge, Louisiana

Computer Telephony Systems Specialist, 1998 - 2002

- Provide on-site support for all equipment and software related to Hamilton's Baton Rouge, Louisiana relay center and all administrative hardware and software
- Assist in developing and troubleshooting software for Hamilton's relay services

The Village at Breckenridge, Wyndham Resort – Breckenridge, Colorado

System Administrator, 1991 – 1998

- Maintained Unix based file server
- Provided first-line software support for server including interfaces to in-room video system, video check-out system, PBX system, call accounting system and point of sales system in the resort's bars and restaurants.
- Provided software solutions to management and training to users
- Provided support as needed for PBX switch
- Produced short range occupancy forecasts to assist in the development of staffing projections
- Facilitated booking and scheduling of ground transfers and car rentals

PBX Operator, Front Desk Clerk, Relief Night Auditor

- Coordinated four to eight hotel switchboard operators
- Arranged schedules, answered phones, and provided special customer support as needed

- Performed end of day bookkeeping functions as needed.

Hamilton Telephone Company – Aurora, Nebraska

Computer Programmer/Consultant, 1987 – 1991

- Developed and implemented a CAD/CAM system
- Researched existing systems, purchased equipment and customized software to render it compatible with established mapping formats
- Developed a dBase IV application shell to provide database system that enabled telephone operators to provide directory information services

CERTIFICATIONS, CURRENT AND PAST POSITIONS

- Nebraska Telecommunications Association Board of Directors – Since 2006
- Nebraska Telecommunicators Association – Past President
- Edgerton Explorit Foundation Board of Directors - President

EDUCATION

Southern Methodist University – Dallas, TX
B.A. History – 1991

REFERENCES

Eric Carstenson
President, Nebraska Telecommunications Association

Diane Keller
Chief Executive Officer, Memorial Community Health

Sen. Curt Friesen
34th Legislative District, Nebraska Unicameral Legislature

Gary Warren

1006 12th Street, Aurora, NE, 68818 · (402) 694-7237 · gary.warren@hamiltontel.com

PROFESSIONAL PROFILE

30+ years in leadership of diversified telecommunications, business development, government regulation, senior leadership. Gary's core competency is new business development with a particular emphasis and set of expertise in businesses which combine telecommunications, software development and information technology.

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, NE

Senior Consultant, Nedelco Inc d/b/a Hamilton Telecommunications., 2019 - Present

- Lead liaison and representative for Hamilton NG911, Inc.
- Sr. Consultant of seven owned subsidiaries of Hamilton Telecommunications.

Hamilton Telecommunications – Aurora, NE

President, Nedelco Services Corporation, 2003 - 2019

- Secretary-Treasurer of Hamilton Telecommunications and its seven subsidiaries.
- Lead representative for Hamilton NG911, Inc.
- Member of Senior Leadership Team of Nedelco, Inc. d/b/a Hamilton Telecommunications and all of its subsidiaries including Hamilton NG911, Inc.

Hamilton Telecommunications – Aurora, NE

Executive Vice President of Nedelco, Inc. d/b/a Hamilton Telecommunications, 1988 - 2003

- Oversaw initiatives of strategic growth, service offering expansion, and national footprint.
- Senior management leadership for the startup and development of several Hamilton business lines including Hamilton's entry into the provision of Telecommunications Relay Services in the national marketplace
- Liaison and company representative for regulatory boards, government work groups, etc.

Whitney, Newman, Mersch, Otto and Warren – Aurora, NE

Partner, 1975 - 1988

- General practice of law.
- Emphasis on estate planning, real estate, contracts and business corporations.

CERTIFICATIONS, CURRENT AND PAST POSITIONS

- Nebraska State Bar Association (Member); NebraskaLink Board (Chairman); OPASTCO's Fund for Rural Education and Development (President); Nebraska Telephone Association's Economic Development Committee (Chairman); FCC Telecommunications Relay Advisory Council (Chairman); Nebraska State Chamber (Board Member & Past Chairman); Nebraska Information

Technology Commission (Commissioner); University of Nebraska President's Advisory Committee (Former Member); Nebraska Diplomats (Past President & Board Member).

EDUCATION

University of Nebraska – Lincoln, NE
Juris Doctorate from College of Law – 1974

University of Nebraska – Lincoln, NE
B.S. – Political Science and Government – 1971

REFERENCES

Kevin Colwell
Vice President of CapTel, Inc. and Ultratec, Inc.

Kirk Handrup
Hamilton County Nebraska Sheriff

Robert "Bob" Dunbar
Retired, Former Relay Center Administrator, State of Idaho

Ryan Wineteer

1006 12th Street, Aurora, NE, 68818 · (402) 694-9654 · ryan.wineteer@hamiltontel.com

PROFESSIONAL PROFILE

Results driven manager with a keen eye for sales, onboarding and client experience. 10+ years' experience in surpassing revenue goals and managing dynamic teams. Unique ability to tackle complex projects, delegate and educate within the technological and telecommunications arenas.

PROFESSIONAL EXPERIENCE

Hamilton NG911 – Aurora, NE

Manager, 2017 – Present

- Responsible for the management of the newest division within Hamilton.
- Managing the $1 million annual budget of a start-up while working to obtain new revenue streams for the company.
- Oversee two direct reports, seven indirect reports, establishing teaming arrangements with strategic market partners, managing a 24 state marketing and outreach campaign while aligning actions with the vision of the senior leadership team and board of directors of the company.

Hamilton Telecommunications – Aurora, NE

Sales & New Business Development Manager, 2016 – Present

- Promoted to Sales & New Business Development Manager.
- Managed a team of two sales staff.
- Sales growth and focus on enhancing / refining the onboarding and training process for sales staff at Hamilton.

Hamilton Telecommunications – Aurora, NE

Sales & New Business Developer, 2011 – 2016

- Responsible for sales of Hamilton service offerings including circuits and data transport, managed hosting and cloud services, network administration contracts, unified communications services, network hardware, security cameras and VMS software suites.
- Exposed to a wide range technology enhanced personal knowledge to include a strong understanding of most business technology services.
- Grew revenues originating from the sales division fourfold to over $1.6 million annually.

Paul Johnson Office – Lincoln, NE

Agency Sales Associate, 2007 – 2011

- All facets of insurance sales and service, prospecting for new business, and marketing the agency.
- Licensed in the State of Nebraska to sell property, casualty, life and health insurance.
- Produced 70% of the new business for the agency; a level of production unmatched during the 15 years of Paul's agency.

EDUCATION

Wayne State College – Wayne, NE
Masters of Business Administration, 2008 – 2010

- GPA: 3.56

Chadron State College – Chadron, NE
Bachelor of Science in Education, 1999 – 2004

- GPA: 3.86

REFERENCES

Dennis Ferguson
Regional President, Heartland Bank

Chris Holliday
IT & Corp. Operations Manager, Aurora Cooperative

Dr. Ryan Raemaekers
M.D., CHI Health St. Francis

Dixie J. Ziegler

1006 12th Street, Aurora, NE, 68818 · (402) 694-5101 · dixie.ziegler@hamiltonrelay.com

PROFESSIONAL PROFILE

25 years of corporate leadership and national division operational management experience at the forefront of the telecommunications and accessibility arenas. A dynamic leader of teams and innovative accessibility advocacy and solutions. Curator of national branding and identity for Hamilton Relay Services division.

PROFESSIONAL EXPERIENCE

Hamilton Telecommunications – Aurora, NE

Director, then Vice President of Relay Services, also serving as Chief Operations Officer, 1994 – Present

- Responsible for the management of all areas of the Relay business line including operations, marketing, account management, and technical services.
- Responsible for financial outcome of this business line, including profit and loss for its operations.
- Directs operational manager to ensure appropriate and profitable staffing while maintaining high quality service.
- Directs technical manager to ensure operation 24 hours a day and that competitive products are released to the market place in a timely fashion to increase overall usage of Hamilton Relay.
- Directs marketing manager to ensure fulfillment of all state outreach requirements and to ensure that national marketing efforts increase overall usage of Hamilton Relay.
- Directs account manager to ensure all FCC and state contract requirements are met.
- Provides timely, concise and accurate reports to senior management and the Company's Board of Directors.
- Manages the overall business line in a manner consistent with corporate policies, procedures and principles.
- Communicates on a consistent basis through various mediums with all Hamilton
- Telecommunications managers.
- Performs corporate development activity to continue the growth of the division. Researches and recommends new features and services.
- Coordinates with Human Resource Manager to ensure that personnel and human resource issues are handled proactively and on a timely basis.

ORGANIZATIONS

- Served on the National Exchange Carrier Association (NECA) Relay Advisory Council
- Served on the Consumer Advisory Committee (CAC) of the Federal Communications Commission
- Aurora Chamber of Commerce - Member
- Disability Access Committee (DAC) of the Federal Communications Commission as chair of IP CTS Working Group - Member
- 4-H Leader

EDUCATION

Dana College – Blair, NE
B.S. – Marketing, Organizational Communications and Print Media

- Valedictorian

REFERENCES

David O'Conner
Attorney, Wilkinson, Barker, Knauer LLP

Claude Stout
Executive Director, Telecommunications for the Deaf and Hard of Hearing, Inc. (TDI)

Ron Bibler
Montana Telecommunications Access Program Committee

Kent L. Claussen

1616 Directors Row Fort Wayne, IN 46808 · (877) 469-2010 · kclaussen@indigital.net

PROFESSIONAL PROFILE

Over 30 years of experience in the IT and Telecom industries with extensive network and programming experience. Professional strengths include:

- Management / Senior Level experience.
- Experience with a variety of systems such as: TCP/IP v4, v6, Unix, and more.
- Fluent in most modern programming languages and methodologies.

PROFESSIONAL EXPERIENCE

INdigital Telecom – Fort Wayne, IN

Chief Technology Officer, 2012 – Present

- Responsible for the engineering, deployment and operation of INdigital's production NG911 offerings.

- Michigan Enhanced 9-1-1 Network ME9 – June 2014 – Renewable
    - Project scope: Creating a diverse and redundant statewide Network for the delivery of Enhanced 9-1-1 calls to PSAP's throughout the State of Michigan. The final configuration uses two redundant and geodiverse Central Office based data centers, with all originating service providers connected to the ESiNet service nodes. A 9-1-1 service agreement was put in place with the authorities having jurisdiction, and the service transitioned from the legacy provider to the statewide ESiNet using IP over fiber.

- ESiNet for NH NG9-1-1 – June 2015 – Renewable
    - Project scope: Creation of statewide ESiNet, i3 Functional Elements and Network operation capabilities throughout the State of New Hampshire. As the ESiNet provider, and working closely with DESC, refined the IP network design to create a multi-carrier, self-healing IP mesh network, with multiple service delivery points, types and methods.

- Indiana Statewide 911 Plan – 2004 - Renewable
    - Project Scope: Build a cooperative and collaborative mechanism for the advancement of wireless 9-1-1. Facilitate the migration of Indiana's PSAPs to NG9-1-1 capability. This work included the concept, design, implementation and operation of transitional E9-1-1 to pre i3 911 systems that evolved to an i3 compliant NG9-1-1 ESiNet. The network supports all legacy and emerging industry standards, both NENA and ATIS RFAI.

Enhanced Telecommunications Coprporation (ETC) – Sunman, IN

Chief Technology Officer, 2008 – 2012

- Responsible for the engineering and network resources for the company and its subsidiaries in financial, operational and planning capacities.
- Leader of engineering staff covering all of ETC's product offerings.

EDUCATION

Purdue University – West Lafayette, IN
Master of Science, Agricultural Economics – August, 1996

Iowa State University – Ames, IA
Bachelor of Science, Agricultural Business – May, 1992

Iowa state University – Ames, IA
Bachelor of Arts, Computer Science – May, 1992

ADDITIONAL SKILLS

- Executive Level Management Experience – 16 Years
- Professional IT Expeience – 26 Years
- Telecom Networks Experience – 23 Years
- Unix Systems Experience – 31 Years
- TCP/IP v4 Experience – 26 Years
- TCP/IP v6 Experience – 10 Years
- Programming Experience – 29 Years
    - Over 35 programming languages used.
- Expert in network design and troubleshooting.
- US Government Security Clearances.

REFERENCES

Ed Reuter
Executive Director, State of Indiana

Leah Missildine
Executive Director, State of Alabama & 9-1-1 Board

David McCartney
General Manager, Peninsula Fiber Network

Mark Grady

1616 Directors Row Fort Wayne, IN 46808 · (877) 469-2010 · mgrady@indigital.net

PROFESSIONAL PROFILE

Over 35 years of experience as a ground-breaking, innovative leader in the Telecom Industry.
Professional strengths include:

- Technical, Operational, Planning, and Management focused expertise.
- Network system design, and technology innovation.
- Cost study planning and rate study design.

PROFESSIONAL EXPERIENCE

INdigital Telecom – Fort Wayne, IN
Founder and President, 1997 – Present

- Established and created a multi-shareholder structure to develop diversified lines of business in the emerging technology sector of telecom.
- Strategic planning, development, operation and successful delivery of emerging technology in latent market areas.
- Implementation of wholly new approaches to government level policy related to core and essential public safety services.
- Architect and oversee the creation of new services in multiple market areas.
- Develop and promote the training and support of industry recognized staff.

ADDITIONAL SKILLS

- Strategic and operational planning.
- Quality delivery management.
- OA&M, Central Office technologies – (transmission and switching).
- Technical development and management.
- Regulatory policy, compliance and modernization policy.
- Engineering oversight.
- Market segmentation.
- Director, officer and consultant to several other related investments and companied associated with New Paris Telephone (INdigital's founding company).

REFERENCES

Ed Reuter
Executive Director, State of Indiana

Leah Missildine
Executive Director, State of Alabama & 9-1-1 Board

David McCartney
General Manager, Peninsula Fiber Network

Eric R. Hartman

1616 Directors Row Fort Wayne, IN 46808 · (877) 469-2010 · ehartman@indigital.net

PROFESSIONAL PROFILE

Nearly two decades of experience in the IT industry at both entry and management levels. Professional strengths include:

- Field, tech and customer service supervision.
- In-depth understanding of technical programs and their latest developments.
- Support and managing projects from zero to 33% market share, with value per customer in excess of $500k.

PROFESSIONAL EXPERIENCE

INdigital Telecom – Fort Wayne, IN
Executive Vice President, 2007 – Present

- Overall business development.
- 9-1-1 product management.
- Lead service support team.
- Supervise field services team, sales, service managers and trainers.
- Specialize in strategic corporate and customer relations, satisfaction, retention and development.
- Coordinate and lead public relations opportunities for Indiana 911 Board.

Brightnet – New Paris, IN
Product Manager, 2005 – 2006

- Managed a company division.
- Oversaw transition from legacy telephone services to VOIP.
- Supervised deployment of Metaswitch, new PBX systems and Goshen Fiber Network.

INditigal Telecom – Fort Wayne, IN
Data Service Technician, 2001 – 2004

- Entry level position working with VOIP, IP Routing, Class 4&5 Switching, and more.

EDUCATION

Tri-State University – Angola, IN
BSBA in Computer Science and Minor in Business Administration – 2001

ADDITIONAL SKILLS

- IP Avaya Certification.
- Cisco CCNA Training.
- Licensed and Unlicensed Wireless Networking.
- Linux Server Management.

- Samsun PBX and Asterisk PBX.
- Network Monitoring.

REFERENCES

Ed Reuter
Executive Director, State of Indiana

Leah Missildine
Executive Director, State of Alabama & 9-1-1 Board

David McCartney
General Manager, Peninsula Fiber Network

Sean Lehman, GISP, ENP

601 W. Saint Germain St. · (888) 436 – 2666 · geo-comm.com/

PROFESSIONAL PROFILE

As a GIS Project Manager, Sean is responsible for the development, management, and delivery of internal and external GIS consulting, training, and project management services for GeoComm. He has expertise in client communication, project-level satisfaction, and client project needs. In addition, Sean has sales experience selling GIS services to new and existing clients. He has achieved Geographic Information Systems Professional (GISP) certification with 14 years' experience using latest industry standard GIS software and databases working in both private and public sectors.

PROFESSIONAL EXPERIENCE

Geo-Comm, Inc. – St. Cloud, MN
GIS Project Manager, 2014 – Present

GIS Data Resources, Inc. (GDR) – San Rafael, CA
GIS Technical Project Manager, 2008 – 2014

General Dynamics – FallS Church, VA
GIS Analyst, 2006 – 2008

William Lettis & Associates, Inc. – Walnut Creek, CA
GIS Analyst, 2007

Nelson/Nygaard Consulting Associates – San Francisco, CA
GIS Specialist, 2001 – 2006

Gilmore & Associates – New Britain, PA
GIS Specialist, 2000 – 2001

PROJECT EXPERIENCE & EXPERTISE

- South Dakota Next Generation 9-1-1 (NG9-1-1_ System.
  - GIS Workflow Development and Training
- Vermont Next Generation 9-1-1 (NG9-1-1) System.
  - Maintenance Workflows
  - GIS Managed Services & Training
- Professional expertise utilizing ArcGIS in the SDE Environment and integrating/manipulating data in SQL Server 2005/2008 using T-SQL.

- Leading project teams in GIS data analysis and GIS data development for use in public safety dispatch, Computer Aided Dispatch (CAD), and Next Generation 9-1-1 (NG9-1-1) software solutions.

- Overseeing and managing GIS staff on Enhanced 9-1-1 (E9-1-1) CAD GIS data builds throughout the United States.

- E9-1-1 GeoFile builds in accordance to National Emergency Number Association (NENA) guidance, client needs, and specific CAD schema requirement needs with all top tier vendors.

- Consulting, developing, and training clients on GIS workflows and standard operating procedures for public safety.

- Training clients on the use of public safety GIS solutions.

- Consulting with clients to develop and document appropriate Quality Control (QC) plans for accuracy and completeness of GIS data used for public safety purposes.

- ArcGIS 10.2 (Desktop), Geodatabase: (SDE, File, Personal) Geo-processing Tools.

- ArcSDE 9.3, 10.0 Personal ArcSDE Server.

- Extensions: Network Analyst, Spatial Analyst, 3D Analyst.

- SQL Server 2008, T-SQL.

- Access, VBA for ArcGIS, Avenue, AML.

- Trimble Recon XC and Garmin GPS.

- Adobe Illustrator, MaPublisher, AutoCAD, GeoPlan (Permit Software), SPSS.

CERTIFICATIONS

- Geographic Information Systems Professionals (GISP)
- Emergency Number Professional (ENP)
- NENA Workgroup Member
    - Site/Structure Address Points
    - New York State 9-1-1 NENA
- Bay Area Automated Mapping Association (BAAMA)

EDUCATION

West Chester University of Pennsylvania – West Chester, PA
B.A. in Geography

College of Martin – Kentfield, CA
A.A. in Health and Physical Education

Veteran United States Army – Fort Polk, LA
Honorable Discharge

REFERENCES

Lee Ann Magoski
Director of Emergency Communications, Monterey County

Troy Chronister, PMP, CSM
Project Manager, Baltimore County Office of Information Technology

David Bonini, PMP
Project Manager, Tyler Technologies, Inc. – Public Safety Division

Hanna Lord

601 W. Saint Germain St. · (888) 436 – 2666 · geo-comm.com/

PROFESSIONAL PROFILE

Hanna is responsible for all aspects of managing and directing GeoComm's GIS Services and works with Client Services in support of successful project completion. She currently manages project teams providing NG9-1-1 managed services to GeoComm's client base.

Hanna will help provide the GIS team's supervision for this project. This responsibility includes attending project kickoff meetings, assisting with ongoing training of current and new employees, monitoring schedules and providing updates to the project team, providing timely project status reports, and ongoing Quality Control (QC) of data.

PROFESSIONAL EXPERIENCE

Geo-Comm, Inc. – St. Cloud, MN
GIS Manager & GIS Specialist, 2013 – Present

Adam McArthur Agency American Family Insurance – St. Cloud, MN
Licensed Agent Assistant, 2013

Ken K Thompson Jewelry – Bemidji, MN
Sales Coordinator, 2010 – 2013

Pro-West & Associates, Inc. – Walker, MN
GIS Technician, 2010 – 2011

Paul Bunyan Telephone Cooperative – Bemidji, MN
Engineering Intern / Special Project Assistant

PROJECT EXPERIENCE & EXPERTISE

- Developing, managing, and supervising GIS Services with the goal of timely, successful and profitable projects.
- Developing, gaining approval of, and implementing goals and objectives for all areas of responsibility.
- Ensuring cross company GIS knowledge, and managing and supervising GIS Coordination.

- Establishing and maintaining reports pertinent to department activities and providing to President as needed.

- Operating within the NG9-1-1 team to develop and improve processes for current and future projects.

- Enrolled in courses to further knowledge on current processes to better prepare for future projects.

- Constantly working to better understand every aspect of NG9-1-1.

- Providing information and guidance to proposal and sales staff in understanding GIS services.

CERTIFICATIONS

- ESRI, Building Models for GIS Analysis Using ArcGIS, 2014
- ESRI, Basics of Python, 2014
- ESRI, Basics of the Geodatabase Data Model Training, 2010
- ESRI, Creating, Editing and Managing Geodatabases for ArcGIS Desktop, 2010
- ESRI, Working with Geodatabase Subtypes and Domains, 2010

EDUCATION

Bemidji State University – Bemidji, MN
B.S. Geography

REFERENCES

Aaron Fisk
Vice President of Quality, Regulatory and Employee Engagement, Microbiologics

Gregory Galarneau
Owner, Amplifico Consulting Group, LLC

Rebecca Clobes
Business Development Manager, Anderson Center for Management and Leadership Development

Jodi Wroblewski, PMP

601 W. Saint Germain St. · (888) 436 – 2666 · geo-comm.com/

PROFESSIONAL PROFILE

Jodi started with GeoComm as an Agile Product Owner. In that role, Jodi worked with agile teams developing software applications for the public safety industry and was the liaison between product management and software development. She was responsible for creating a collaborative environment across the entire team including Architect, development team, testing, documentation, and Product Manager.

In her current role as an Implementation Manager, Jodi is responsible for managing resources focused on implementation of GeoComm software products, assuring installation and training services provided by the GeoComm Implementation team are completed in a timely manner and exceed customer expectations.

PROFESSIONAL EXPERIENCE

Geo-Comm, Inc. – St. Cloud, MN
Implementation Manager & Agile Product Owner, 2019 – Present

Netgain Technology – St. Cloud, MN
Director of Client Implementation, Professional Services, & Project Management, 2016 – 2018

St. Cloud State University (SCSU) – St. Cloud, MN
PMO Manager / Project Manager & Technology and Marketing Administrator, 2012 – 2016

ProcessPro Software, St. Cloud, MN
Implementation and Support & Project Manager / Account Manager, 2007 – 2012

Short Elliott Hendrickson (SEH), Inc. – St. Cloud, MN
Assistant Project Manager / Administrative Technician, 2004 – 2007

PROJECT EXPERIENCE & EXPERTISE

- Managing daily activities of the Implementation division for projects and employees assigned.
- Ensuring project reporting is done in a timely manner.
- Providing implementation project management support, assisting Implementation Specialists with more complex projects and customers.
- Providing project communication to internal and external stakeholders.

- Monitoring the progress of high-profile client projects and ensuring issues are resolved in timely manner.
- Guiding development and ensuring training for business partners and VARS.
- Assisting in the development and refinement of installation materials and processes.
- Assisting with Product Verification (PV) lab development, maintenance, and standard operating procedures.
- Ensuring smooth transition of software implementation projects to the support team.
- Successfully attaining Key Performance Indicators (KPI).
- Developing and maintaining working knowledge of GeoComm software products.
- Developing and maintaining working knowledge of 9-1-1 technologies and standards.
- Developing and maintaining a working knowledge of 3rd party software applications used with GeoComm products.
- Maintaining technical knowledge of all aspects of how GeoComm products connect in a variety of installation environments to include cloud computing, various computer hardware, software, networking configuration, database technologies, and wireless communications .
- Maintaining a working knowledge of client/server operations, ArcGIS Server, ArcSDE, geodatabases, Windows Server, Linux, Docker, SQL Server and other commercial DBMS Platforms, IIS, Active Directory, Network Routing, XML, Web Services, and other related software applications and principles.

CERTIFICATIONS

- Project Management Professional (PMP), 2016
- Data Security Awareness Training and HIPAA HiTech and Privacy, 2016
- Supervisor Development Certificate Program, 2016
- St. Cloud State University Performance Award, 2015 & 2016
- MnSCU IT Department Performance Award, 2015 & 2016

EDUCATION

Augsburg College – Minneapolis, MN
B.A. Communications with Public Relations Emphasis

REFERENCES

Casey Gordon
Chief Information Officer, College of St. Benedict and St. John's University

Dough Schick
Director of Client Services, Americas Merrill Corporation / Datasite

Jodi Kuznia
Director of Research and Development, St. Cloud State University

John Browning, PMP

2323 W 5th Avenue Columbus, OH · (888) 800-4003

PROFESSIONAL PROFILE

Mr. Browning is a veteran member of the DDTI NG911 Implementation Team. He has assisted in the deployment of DDTI's NG911 suite in Ohio, Massachusetts, and various other testing and staging environments. He has coordinated regular software upgrades in Massachusetts and written multiple Implementation and Test Plans to document the work required. Mr. Browning is a certified Project Management Professional (PMP).

PROFESSIONAL EXPERIENCE

Digital Data Technologies, Inc. (DDTI) – Columbus, OH
Systems Implementation Coordinator, 2016 – Present
System Implementation Engineer, 2014 – 2016
E911 Support and Implementation, 2007 – 2014
GIS Analyst, 2005 – 2007

EDUCATION

Ohio State University – Columbus, OH
Bachelor of Science, Natural Resources – 1994

REFERENCES

Pat Neville
Release Manager, Safety & Security Technologies | Comtech Telecommunications Corp

Johnathon Voegeli
Senior Systems Engineer, Synergem Technologies, Inc.

Melissa French
Associate Configuration Analyst, Safety & Security Technologies | Comtech Telecommunications Corp

Tony Collura, PMP

2323 W 5th Avenue Columbus, OH · (888) 800-4003

PROFESSIONAL PROFILE

Mr. Collura has been with DDTI since 2000 and is a veteran member of the DDTI Data Creation and Production Team. He has contributed to over 50 GIS data normalization projects and is the project lead for NG9-1-1 implementation in St. Louis County.

PROFESSIONAL EXPERIENCE

Digital Data Technologies, Inc. (DDTI) – Columbus, OH
Director of Operations, 2014 – 2018
Project Manager, 2006 – 2014
GIS/GPS Analyst, 2000 - 2006

EDUCATION

Ohio State University – Columbus, OH
Bachelor of Arts Urban and Regional Geography, 2000

ADDITIONAL SKILLS

- Certified Project Management Professional (PMP)

REFERENCES

John Walsh
Vice President, Safety & Security Technologies | Comtech Telecommunications Corp

Josh Plew
911 Services Coordinator, St. Louis County ECC

Marty Ham
Project Manager, Safety & Security Technologies | Comtech Telecommunications Corp

Tessa Haizel-Cobbina

2323 W 5th Avenue Columbus, OH · (888) 800-4003

PROFESSIONAL PROFILE

Mrs. Haizel-Cobbina is currently part of the Location Database (LDB) Services team at DDTI. She managed the process of transitioning service providers and PSALI customers from their existing ALI Database systems to the DDTI LDB in Massachusetts and Ohio. She is part of a team that oversees updates to the LDB, coordinates discrepancy workflows, and provides support to the PSAP.

PROFESSIONAL EXPERIENCE

Digital Data Technologies, Inc. (DDTI) – Columbus, OH
LDB Services Coordinator, 2018 – Present
LDB Engineer, 2014 – 2018

Arrow Electronics, Inc. – Centennial, CO
Database Analyst, 2007 – 2014

EDUCATION

DeVry University, Keller Graduate School of Management – Naperville, IL
Master, Information Systems Management – 2015

DeVry University – Naperville, IL
Bachelor of Science, Computer Information Systems - 2005

REFERENCES

Glenn Roach
Program Director, NGCS, Motorola Solutions

Edgar Goroza
System Engineer, Safety & Security Technologies | Comtech Telecommunications Corp

Charles Ashworth
System Analyst, Massachusetts State 9-1-1 Department

Craig Hamm

2323 W 5th Avenue Columbus, OH · (888) 800-4003

PROFESSIONAL PROFILE

Mr. Hamm currently supports the DDTI NG911 system in Massachusetts as the primary System Engineer. His responsibilities include the design, implementation, and monitoring of the telemetry infrastructure as well as providing tier 2 support for the DDTI NG911 services. He has coordinated regular software upgrades in Massachusetts and written multiple Implementation and Test Plans to document the work required. Mr. Hamm holds several certificates, including the Microsoft Certified Solutions Expert (MCSE) for Server Infrastructure and the Microsoft Certified Solutions Associate (MCSA) for Windows Server.

PROFESSIONAL EXPERIENCE

Digital Data Technologies, Inc. (DDTI) – Columbus, OH
System Engineer, 2018 – Present
Support Manager, 2014 – 2018

The Echo Group – Conway, NH
Senior Systems Administrator, 2009 – 2014

XAKTsoft, Inc. – Powell, OH
Senior Systems Administrator, 2002 – 2009

UUNET / World Comm – Ashburn, VA
Network Engineer III, 1999 – 2002

EDUCATION

Ohio State University – Columbus, GA
Bachelor of Science, Music Education – 1999

REFERENCES

George Manso
Security Director, Safety & Security Technologies | Comtech Telecommunications Corp

JT Williams
Senior Network Engineer, Safety & Security Technologies | Comtech Telecommunications Corp

Christopher Mangiarelli
Principal Systems Engineer, Safety & Security Technologies | Comtech Telecommunications Corp

Mitch Pinkston, PMP

2323 W 5th Avenue Columbus, OH · (888) 800-4003

PROFESSIONAL PROFILE

Mr. Pinkston is a veteran member of the DDTI Team. He has managed the statewide deployment of an i3 compliant NG9-1-1 system for DDTI. In addition, Mr. Pinkston oversaw the transformation of the DDTI Operations department to align with NG9-1-1 requirements.

PROFESSIONAL EXPERIENCE

Digital Data Technologies, Inc. (DDTI) – Columbus, OH
Chief Information Officer, 2018 – Present
Operations Manager, 2014 – 2018
Project Manager, 2010 – 2014
GIS/GPS Analyst, 2003 – 2010

EDUCATION

Bowling Green State University – Bowling Green, OH
Bachelor of Arts in Geography, 2003

ADDITIONAL SKILLS

- Certified Project Management Professional (PMP)

REFERENCES

Bill Mikucki
Vice President of Technical Operations, Safety & Security Technologies | Comtech Telecom. Corp

Peter Grace
GIS Analyst, Massachusetts GIS Department

Norm Fournier
Deputy Executive Director, Massachusetts State 911 Department

Chris Johnson

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

A proven leader who is detail oriented, dedicated and driven to succeed in the challenging and fast paced field of Communication. Over 20 years of experience in Field and Network Operations, Project Management, Telecommunications and Leadership roles.

- Proven background in competing in the regulated ILEC arena as well as non-regulated, highly competitive middle-mile sector.
- Extensive knowledge of the OSP, ISP, Engineering, Transport, Pricing, OAM, Process creation, Business Continuity, Business Development & Operational software.
- Strong problem solving, conflict resolution and leadership skills.
- Confident performing under extreme pressure in the ever-changing landscape of the communications industry both regulated and non-regulated.
- Ability to create and maintain key relationships within our industry for the purpose of synergy and personal development.
- Develop and promote talent within the organization and recruit new talent.
- Excellent Project Management skills that allow me to keep several projects moving forward simultaneously.

PROFESSIONAL EXPERIENCE

NebraskaLink – Lincoln, NE

Director of Operations, 2016 – Present

- Responsible for a staff of 27 within the Operations Department that includes Network Engineering, Provisioning, OSP, Service Assurance, NOC/Support & IT.
- Create & Implement Operation process and procedure.
- High level Sales Engineering and Business Development roles.
- Contract and RFP review for onboarding new customers and bidding opportunities.
- Creating and Maintaining Operations yearly Capex and Net OPS budget.
- Creating and Maintaining Operations 1, 3- & 5-year strategic goals.
- Opportunity bidding and customer circuit pricing based off those and many other factors.
- New vendor and product selection.
- Work directly with the CEO, CFO & VP as part of the Senior Leadership Team for strategic planning, company financial health and company policy.

Director of Fiber Optic Networks and Network Assurity, 2013 – 2016

- Responsible for all customer facing Operations tasks.
- Network assurance tasks to include preventative maintenance, locating services and vendor contracts.
- Service Assurance tasks for ensuring timely delivery of services.
- OSP design and engineering.
- Customer installs, testing and closeout packages.
- Process creating and implementation.

Outside Plant Manager, 2011 - 2013

- Responsible for a 450-mile project funded by BTOP to complete NLK's statewide middle-mile network.
- Created and maintained all records for the federal BTOP program.
- Managed all construction, splicing and engineering contractors.
- Finished the $16M project early and only 1% over budget.
- Created OSP budget.

Plainview Telephone Company
Outside Plant Manager, 2007 - 2011

- Responsible for overseeing 100% FTTH project
- Responsible for OSP budget.
- Vetting and selection of FTTH vendors.
- Part of a 4-person leadership team.
- Created and maintained OSP processes and procedures as it pertained to the new deployment of FTTH.

Pierce Telephone Compnay
Combination Technician, 2000 - 2007

- Performed all aspects of fiber and copper underground construction.
- Performed all switching and service updates to one of two DMS-10 switches.
- Installed all first gen DSL, dial-up internet, I & O and phone system services.
- Preventative Maintenance on all plant, property and equipment.
- Troubleshoot and repair all issue related to above services.

EDUCATION

Mitchell VO – Technical Institute
AAS, Satellite Communications & Telecommunications

REFERENCES

Terry Jacobsen
Field Technician, NebraskaLink

Grant Dummer
General Manager, Plainview Telephone Co.

Jason Axthlem
Vice President of Business Development, NebraskaLink

Brent Timothy Lamb, PMP

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

Forward-thinking and results-driven technology professional with over 23 years of telecommunications operations experience, skilled in developing teams to exceed business objectives. Solid working knowledge of organizational design, operations, technology management, engineering, and construction, including 15 years of managerial responsibility.

PROFESSIONAL EXPERIENCE

NebraskaLink – Lincoln, NE

Operations Manager, 2019 – Present

Responsible for the day-to-day activities of field operations and operations engineers in the design, installation, construction, and maintenance of Ethernet transport facilities, special access, private line, and other optical carrier services.

Key Duties:

- Responsible for company operational metrics, employee performance, and department productivity
- Accountable for operations department and project level budgets
- Direct accountability and management of construction projects and customer order due dates
- Manage service assurance department to ensure a seamless customer experience for service orders
- Project management of customer builds and approved business case construction projects
- Fleet operations

CenturyLink / Quest Communications

Senior Manager LNI Engineering and Construction, 2011 – 2019

Responsible for all local network implementation of engineering and construction operations in NE. Objectives include driving the mass expansion of the fiber network to add depth and breadth of services for large/medium/small enterprises and residential consumers.

Key Duties:

- Project Manage hundreds of capital projects simultaneously to meet required build schedules and budgets for each separate corporate driven fiber (FTTx) initiative, to include: FTTT, FTTP, FTTN, vectoring, GPON, Ethernet-to-business, inter-office facility upgrades, transport, data, and core network additions/upgrades
- Engineer and construct central office and data center core, transport, and access networks to support the increased capacity demands of emerging technologies and to support increased bandwidth
- Design and build fiber backbones, distribution networks, data center infrastructure, central office, and customer prem technology solutions for business and consumer usage
- Manage all state, count, and city/town municipality civil road projects.
- Lead the local engineering and construction operations teams over a three-year period in the design, execution, and construction overbuild to transition 49,000 Omaha homes from a hybrid fiber-coax network to a FTTP architecture with full residential GIG data capacity, delivering the first large

scale digital video services deployment to a metro area in the company, an additional 100k+ video cable homes enabled using FTTN architecture.

Area Plant Supervisor / Supervisor Network Operations & Central Office Technician, 2005 – 2011

Perform all supervisory/management functions (planning, organizing, leading, controlling) for operations in NE and IA.

Key Duties:

- Direct responsibility for managing outside plant crews & facilities, to include project coordination, staffing, resource allocation, scheduling, splicing, and maintenance
- Interface with contractors, vendors, engineers, and construction crews on the design, installation, and implementation of capital technology projects, and provide ongoing maintenance of existing network facilities
- Manage the installation of technology projects and network deployment of fiber, coax, and copper-based services in the central office, data centers, field, and customer premise

Lead Operations Technician, 2001 – 2005

Lead Network Technician for network reliability and maintenance of all DMS & SONUS VoIP switches in the Mountain West Region, and lead fiber PoP technician for the Denver metro area.

Key Duties:

- Manage the day-to-day operations and activities within a highly unique technology operations and data center infrastructure (4-way national fiber juncture, Tera-PoP, Ip backbone, long-haul site)
- Maintain nationwide fiber optic network equipment and facilities
- Experienced on Nortel DMS-100, 250, and 500 telephone switches, Sonus NextGen VoIP switches, Digital Cross Connect Systems, OC-192 and OC-48 configs, optical equipment, long-haul and metro fiber systems, copper cable, Ethernet, and coax technologies
- Expert knowledge of Voice over Internet Protocol (VoIP), Sonet, ATM, DWDM, Metro, Long haul, Cable Systems and associated optical and digital technologies and applications

Intermedia Communications

Unified Voice Technician, 2000 – 2001

Coordinate customer and network upgrades and troubleshoot network equipment, and customer network issues

Key Duties:

- Coordinate customer and network upgrades and planned outages to network equipment
- Work with multiple customers and vendors simultaneously to fix business and residential technology troubles
- Troubleshoot customer and network issues within 30 DMS-500 and 10 DMS-250 telephone switches, in a tier 2 Network Operations Center & call-center environment

United States Air Force

Telephone Systems Technician / Crew Chief, 1996 – 2000

Key Duties:

- Supervisor/crew chief of inside central office and outside I&M crews responsible for all base communications, to include switch, toll, frame, and customer facilities
- Vital member and one of only two telephone operations representatives for the high-performing Simulated Electronic Launch of the Peacekeeper/Minuteman missile (SELP/SELM) team,

providing communications support, test and installation of command post and radio equipment, and acting as the communications expert and point of contact
- Maintain DMS-100 and Raytheon DSS switches and circuits

AREAS OF EXPERTISE

- Operations Management
- Capital and Expense Budgeting
- Construction & Project Management
- Network Design
- Business Development & Administration
- Engineering
- Procurement

CERTIFICATIONS

- Project Management Professional (PMP)

EDUCATION

Amberton University
Master of Business Administration / Management

University of Phoenix
B.S. Business Administration

Community College of the Air Force
Associate of Applies Science in Electronic Systems Technology

REFERENCES

Aaron Krebs
Application Engineer, Clearfield

Dan Kaiser
Director of Engineering & Construction, CenturyLink

Glenn Winham
Manager of Engineering & Construction, CenturyLink

Marissa Munch, PMP, PMI-ACP

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

- Certified Project Management Professional with 10+ years telecommunications project experience
- Experience leading and coordinating teams
- Adapt at cross-cultural professional communication

PROFESSIONAL EXPERIENCE

NebraskaLink – Lincoln, NE

Service Assurance / Project Manager, 2018 – Present

- Manage 100+ ongoing circuit implementation orders for milestone scheduled completion and communicate status to stakeholders
- Enhance customer experience by creating automatic milestone notifications, providing immediate status
- Provide priority customer support for clients
- Develop automated on-time performance and cycle time reports to identify timeline jeopardies and missed milestones to allow immediate managerial coaching
- Develop daily upcoming and past due task list reports to provide visibility into priorities
- Cross-departmental process creation for non-standardized order tracking

Alorica

Program Manager, 2015 - 2018

- Managed USPS upgrade project from AVPN to Ethernet encompassing 10,000 site locations
- Directed FAA 1,800 site install project with high risk potential, air traffic control impact
- Provide guidance and improvement suggestions for 15 direct reports managing installation of AT&T business data and voice circuits
- Increased on-time schedule completion through whole team milestone reviews and coaching, repeatedly exceeding the 90% monthly goal
- Negotiated network backlog completions on a VP level allowing dependent project release and increased customer satisfaction evidenced through increased sales
- Building-wide morale project manager including yearly summer festival and monthly smaller-scale activities

West Corporation

Program Manager, 2013 - 2015

- Managed implementation of Opt-E-Man, Gigaman & ASE switched ethernet product services for AT&T business customers, primarily government offices, resulting in 200% upgraded data bandwidth
- Coached, supported, and guided 5 area managers in team development
- Compiled performance data, identified areas of improvement, and created action plans
- Coordinated development of client process standards
- Collaborated with network partners to improve process and efficiencies
- Participated in job fair events to improve brand and talent acquisitions

Project Support Coordinator, 2011 - 2013

- Developed and implemented local services agent-level order training for overseas partner related to a new business model allowing cost of labor decreases by 74%
- Supported offshore and domestic services as a subject matter expert, including overseas travel
- Examined weekly reports to ensure monthly metric goals were exceeded
- Hosted monthly knowledge sharing and training calls

Project Manager, 2007 – 2011

- Applied elements of project management plan to manage delivery of data circuits for business customers
- Located and resolved any issues that could potentially delay orders
- Developed strategic relationships with key stakeholders
- Schedule management, risk management
- Designated lead on Bank of America project installing 1,000 locations

CERTIFICATIONS

- Project Management Professional, 2017
- Certified Telecommunications Network Specialist (CTNS), 2018
- Project Management Institute – Agile Certified Practitioner, 2019
- MEF Carrier Ethernet Certified Professional, 2019

PRESENTATIONS

- Project Management Changes for an Evolving Environment: PMBOK 6 Updates and Exam Changes – PMI Luncheon, Omaha, NE, November 2019

EDUCATION

University of Nebraska at Omaha – Omaha, NE
B.S. Business Administration Specializing in Marketing

REFERENCES

Susan Dodds
Senior IT Infrastructure Support Analyst, State of Nebraska

Julie Kortus
Project Manager, Office of Chief Information Officer, State of Nebraska

Tom Flair
WAN Network Engineer, University of Nebraska

Mark G. Shaw

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

A hands-on Chief Executive Officer with expertise in business development, operations, OSP engineering, software systems, and sales.

PROFESSIONAL EXPERIENCE

NebraskaLink Holdings, LLC – Lincoln, NE

CEO, 2014 – Present

- Responsible for creating, and fine tuning the strategic short-and long-term goals of the company.
- Maintain communication and updates to the Board of Directors.
- Creates an environment and culture that focuses on fulfilling the company's mission, vision, and values.
- Oversees the operational management of all departments.

Director of Business Development/Carrier Sales, 2011 – 2014

- Develop the Wholesale Division to include obtaining vendor certifications, negotiating Master Service Contracts and Service Level Agreements, and creating responses for Requests for Proposals (RFPs, RFIs, RFQs).
- Established direct fiber interconnects with national, local and wireless carriers.
- Designed and implemented the tools and processes for tracking customer inventories, circuit data/DLRs, underlying carrier data to include financial data for easy expense verification, profitability reporting, and forecasting

South Dakota Network, LLC – Sioux Falls, SD

Director of Pricing, Provisioning, and Optimization, 2009 – 2011

- Work with vendors in order to find more cost effective or diverse solutions into existing or new markets.
- Reduce expenses through leased network design, consolidation, or volume negotiations.
- Use business process redesign to reduce operational costs, find ways to improve customer service, and improve the time to market products.

Senior Manager of Pricing and Provisioning, 2004 – 2009

- Responsible for ensuring the best price and design of leased network capacity and creating pricing for commercially sold services.
- Established pricing for new or unique product offerings and helping prepare RFP responses.
- Created and documented pricing methods, tables and contractual requirements to improve accuracy and reduce timing response.

Manager of Network Provisioning, 2004 – 2004

- Help develop the Project Management skills of employees for use on larger network projects.

- Responsible for the design and install of DSO, DS1, DS3, and OC-n level circuits as well as Frame Relay, ATM, Ethernet, and MPLS services.
- Monitor network and equipment capacities and ensure proper diversity is maintained through the network.

OSP Engineer/Project Manager/Provisioning Engineer, 1998 – 2004

- Contracted directly with vendors and was the project manager for all fiber construction and splicing.
- Engineered fiber construction projects to include compliance with all local and state requirements.
- Designed voice and data circuits through the network.

Cable and Wireless USA – Akron, OH
1997 – 1998

MCI – Cleveland, OH
1996 – 1997

United States Air Force – Fairbanks, AK
1992 – 1996

CERTIFICATIONS

- PMP Certified, PMI – 2005

EDUCATION

Capella University
Bachelor of Science in Business Administration, 2005
Cum Laude

Community College of the Air Force
A.A.S. Electronic Systems Technology, 1995

Six Sigma Green Belt, Villanova University – 1994

REFERENCES

Charles Fast
Vice President, Consolidated Companies, Inc.

Mark Shlanta
Chief Executive Officer, SDN Communications

Tom Rolfes
Project Lead Network Nebraska & Education Information Technology Manager, State of Nebraska

Chad Tracy

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

20+ years of experience in Telecommunications:

- Experience with the installation and repair of: DWDM, Ethernet, MPLS, SONET, TDM
- Direct experience with: Accedian, Adtran, Adva, Brocade, Calix, Ciena, Cisco, Fujitsu, Juniper
- Ability to work independently
- 5+ years of supervisor experience
- Excellent customer service skills
- Experienced with Microsoft office products (Word, Excel, Power Point, Visio, etc.)

PROFESSIONAL EXPERIENCE

NebraskaLink – Lincoln, NE

Engineering Manager, 2015 – Present

Currently managing a department of Engineers and Technicians that are responsible for: circuit turnup (design, provisioning and testing), troubleshooting of customer circuits, and network augmentation. Evaluated existing procedures and made proactive adjustments to meet changing demands. Provided technical leadership for company to effectively steer strategic plans and future projects.

Network Engineer

Preformed: configuration, design, and support for a DWDM fiber optic network. Handled enterprise and wholesale carrier circuits: design, provisioning, turn-up, and repair. Implemented a circuit database for designs and an order workflow system that improved; order turn up efficiency, maintenance notification accuracy, and design record upkeep. Monitored network capacity and performance, as well as diagnosed and resolved complex network problems.

Kansas Fiber Network – Wichita, KS

Transport Engineer, 2012 – 2015

Supported a statewide fiber network interconnecting various ILECs and wireless carriers. Responsibilities included turn up, testing and repair of Layer 2 Ethernet, TDM and SONET circuits, configuration, installation and maintenance of fiber optic equipment. Developed practices and procedures for testing acceptance and maintenance routines.

CenturyLink – Bentonville, AR

Network Operations Tech II, 2009 - 2012

Remote technician assigned 150 miles of unground fiber and 5 POP sites. Completed daily locating of unground fiber routes, maintenance of POP sites (battery plant, environmental alarms etc.) and the turn up, test and repair of carrier circuits (DS1/DS3, Ethernet, and SONET). Lead technician for Wal-Mart's three most important data centers in the Bentonville/Rogers area.

Cox Communications – Topeka, KS
Transport & Data Tech II, 2004 – 2009
Provided technical expertise in commercial data and voice services in the northern Kansas area. Senior Technician charged with the responsibility of meeting project deadlines, providing general guidance/direction, training, and technical assistance to junior level support personnel. Experienced in the installation and testing of: DS1, DS3, Ethernet, and SONET circuits. Performed the installation, configuration and maintenance of: Cisco, Fujitsu, Juniper, Terrawave/Calix, and other equipment.

Southwestern Bell Telephone – Topeka, KS
Manager Special Services, 1995 – 2004
Supervised a crew of 13 System Technicians in the Lawrence and Kansas City Metro area. Organized the routine maintenance of 675 remote fiber locations and the installation of fiber optic equipment. Preformed presentations to State and Federal legislators, educating them in outside plant and DSL remote equipment.

System Technician
Providing leadership and training in the Wichita metro through experienced maintenance and installation of various special circuits including ISDN, T1, Frame Relay and ADSL services. Duties also included traveling to various SWBT offices to demonstrate installation and educate customer service technicians and sales representatives in ADSL products. Presentations to communications consultants of various universities and corporations throughout Kansas to demonstrate how the potential of ADSL products will meet their growing needs of communications.

CERTIFICATIONS

- Fujitsu FLASHWAVE 4500
- Cisco ONS 15454 CPT
- Cyan Z-Series
- MEF CECP

EDUCATION

IT Technical Institute – Little Rock, AR
AAS, Electronics Engineering Technology

REFERENCES

Jeremy Gorusch
Solutions Engineer | North American Sales, Accedian

Scott Johnson

Jacki Synhorst
CB Transport Support Supervisor, Cox Communications

Don Uhrmacher

3900 NW 12th St. Ste. 100 Lincoln, NE 68521 · (888) 893 - 2185 · nebraskalink.com/

PROFESSIONAL PROFILE

A dedicated and performance-driven telecommunications manager with extensive experience in all facets of network testing and support, budgeting, reports creation, customer support, vendor management, project management and database and hardware administration. Leverages practical experience with strong communication skills, working well with all levels of an organization. Consistently meets goals, demonstrating an ability to achieve maximum effectiveness while maintaining high standards. An analytical evaluator who ensures optimal quality and functionality of networks.

PROFESSIONAL EXPERIENCE

NebraskaLink Holdings, LLC – Lincoln, NE

Service Support Manager, 2018 – Present

- Customer escalations
- Carrier performance reporting
- Customer care for all circuits after turnup

Service Assurance Manager, 2016 – 2018

- Conversion to new inventory program
- Order workflow
- Customer escalations

Precision Utilities Group – Lincoln, NE

Manager, 2015

- Managed contract technicians daily workflow
- Added and removed equipment programmed on customer's accounts
- Tracked equipment being installed
- Interfaced with customers to ensure quick resolution of install or repair issues
- Maintained supply levels to ensure parts were available to complete installs and repairs

WiseConnect – Lincoln, NE

Area Manager, 2015

- Managed contract technicians daily workflow
- Added and removed equipment programmed on customer's accounts
- Interfaced with customers to ensure quick resolution of install or repair issues
- Maintained supply levels to ensure parts were available to complete installs and repairs

Alltel and Windstream – Lincoln, NE

Service Center Manager, 2002 – 2014

- Supervised and provided technical support for network tests and network support.
- Developed yearly budget.

- Provided reports for internal and external customers.
- Set up and hosted conference calls and face-to-face meetings with large national wholesale customers.
- Conversion projects and project management

Service Center Manager, 2000 – 2002

- Maintained customer satisfaction by providing problem-solving resources; managing staff.
- Supervised and provided technical support for network tests, local tests, network support, repair service operators, dispatchers, assigners, facilities.
- Developed yearly budget.
- Provided reports for internal and external customers.
- Researched trouble reports for Nebraska Public Service Commission.

Service Assurance Technical Coordinator, 1999 – 2000

- Maintained the customer repair process by coordinating all work groups in the Service Center.
- Supervised and provided technical support for network tests, local tests, network support, repair service operators, and PBX operators.
- Developed yearly budget.
- Provided reports for internal and external customers.
- Researched trouble reports for Nebraska Public Service Commission.

Network Transport Engineer, 1997 – 1999

- Maintained alarm and testing system integrity by providing engineering and maintenance support.
- Performed NEC alarm system database and hardware administration.
- Coordinate new alarm site installations.
- Build new alarm sites in the database.
- Configure remote alarm units to replace defective equipment.
- Handled Anritsu network test system database and hardware administration.
- Isolated and replaced defective test equipment.
- Completed miscellaneous projects.

Aliant – Lincoln, NE

Assistant Supervisor, Network Operations Center, 1994 - 1997

- Maintained network and circuit integrity by managing technicians and system resources.
- Supervised network test department.
- Prepared outage reports for executive staff.
- Interfaced with switching and transport engineers for trouble resolution.
- Attended face-to-face meetings with major customers.
- Established training priorities.

Lincoln Telephone – Lincoln, NE

Engineering Assistant, Network Operation Center, 1992 – 1994
Project Assistant , Network Transport, 1990 – 1992
Network Switch Technician, 1978 – 1990

CONTINUING EDUCATION

Central Community College:

- *Basic Electricity I*
- *Basic Electricity II*
- *Basic Electronics I*
- *Basic Electronics II*
- *Electronic Communications I*
- *Electronic Communications II*
- *Digital Techniques*

Aliant and Alltel:

- *How to Build a Better Team*
- *Managing Management Time*
- *Nortel Smart Banks*
- *Nortel S/DMS Transport Nodes*
- *Signaling System Seven*
- *Emerging Access Technologies*
- *GTE 91A PCM Carrier Equipment*
- *NEC 21GTX Administration*
- *Wiltron Centralized Maintenance Testing System*
- *Nortel DMS10 Overview*
- *Nortel DMS10 Translations*
- *Nortel DMS100 Translations*
- *GTD#5 Database Records*
- *GTD#5 Translations*
- *GTD#5 Equal Access Translations*
- *Digital Computer Fundamentals*
- *Digital Math*
- *Basic Switchroom Theory and Switch Adjustment*
- *The Evolving Network*
- *Sonet/ATM Network Testing*
- *Tellabs 532L DACS*
- *Telecom Solutions DCD-523 Synchronization*
- *Telecom Solutions IDST*
- *AFC DLC*
- *Microsoft Excel*
- *Microsoft Word*
- *Microsoft NT*

Zenith and Heath:

- *Electronic Test Equipment*
- *CMOS Digital Techniques*
- *Fiber Optics*
- *Data Communications and Networks*
- *Microprocessor*

REFERENCES

Greg Wasson
Operations Coordinator, Union Bank & Trust

Steve Meradith
Regional Vice President of State Government Affairs, Windstream

Jacki Synhorst
State Government Affairs Coordinator, Windstream

HAMILTON APPENDIX 6: HAMILTON NG-SEC COMPLIANCE MATRIX

Next Generation 9-1-1 Security Audit Checklist
Hamilton NG911, Inc.

AUDITOR:
Rob Leonard, Information Security Manager - Hamilton NG911
www.HamiltonNG911.com
NG911@hamiltontel.com
800.821.1831

HAMILTON NG911

Hamilton NG911 NG-SEC Audit Checklist

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: Date: 5/22/2020

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: Date: 5/22/2020

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	Sharing of account information is prohibited
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	

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	

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	

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	

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	

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	

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	

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	

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	

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	

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	All key safeguarding resides on a server

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	

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	

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: Date: 5/22/2020

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	

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	

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	

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	

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	

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	

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	Non Applicale as there has been no intial risk assessment completed on the system
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	Non Applicale as there has been no intial risk assessment completed on the system

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	

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	

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	

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	

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	

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	

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	

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	

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	
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	

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	

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	
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	

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	
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	

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	

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	

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	No personal equipment is used unless requested by customer. Safegurads would then be put in place
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	

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	

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	This plan is currently under development.
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	

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	

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	

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: Date: 5/22/2020

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	

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	

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	

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	

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	

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	

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: Date: 5/22/2020

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: Date: 5/22/2020

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	However, this need can be implemented if necessary for any particular client
214	7.5.5	Are BC/DR drills conducted at least annually?	R	☑ C ☐ No ☐ N/A	

Section 7 - Incident Response Auditor: Date: 5/22/2020

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	

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	

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: Date: 5/22/2020

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	

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	

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	

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	

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	

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	

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	

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: Date: 5/22/2020

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: Date: 5/22/2020

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	

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	

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	

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	

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	

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	

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	

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	

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	

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	

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: Date: 5/22/2020

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	

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	

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: 

Date: 5/22/2020

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	However, the name of the policy is "Hardware Aquisition and Lifecycle Policy" for reference

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	

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	All program changes are tracked in our development management system (JIRA). Change requirements are managed + confirmed through our testing matrix per appropriate manager.
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	Logging systems are incorporated into software and report per type of program in question. Errors outside of "normal operating errors" are sent to tech group w/ an escalation path automatically by logging infrastructure.
350	7.4.4	Are error checking and validation controls are present in software?	R	☑ C ☐ No ☐ N/A	Input validation, exception checking and appropriate failure handling are part of the development standards. Validation controls must be defined + satisfy requirements made during development to pass thru our testing phase of software develpment.
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	

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	

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	
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	
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	

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: Date: 5/22/2020

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	

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	☑ 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	☑ C ☐ No ☐ N/A	
370	6.4.6.1	The TKIP passphrase is non-trivial and meets the requirements of this document?	R	☑ C ☐ No ☐ N/A	
371	6.4.6.1	The rekey maximum is no greater than 3600 seconds?	R	☑ 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	☑ C ☐ No ☐ N/A	

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	☑ C ☐ No ☐ N/A	
374	6.4.6.1	Ad hoc modes are disabled?	R	☑ 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	☑ 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	☑ C ☐ No ☐ N/A	
377	6.4.6.1	Use of Intrusion Detection Systems (IDS) is encouraged on WIFI LANs	BP	☑ C ☐ No ☐ N/A	
378	6.4.6.1	Maximum encryption key lengths supported by the device should be utilized	BP	☑ C ☐ No ☐ N/A	

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	☑ C ☐ No ☐ N/A	
380	6.4.6.1	The default SSID channel should be changed from its default value	BP	☑ 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	☑ 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	☑ 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	☑ C ☐ No ☐ N/A	

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	☑ C ☐ No ☐ N/A	
385	6.4.6.2	If Bluetooth is used is shall be configured to require device identifiers.	R	☑ 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	☑ 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	☑ C ☐ No ☐ N/A	
388	6.4.6.3	Does the entity use the 4.9 MHz band spectrum licensed by the FCC?	R	☑ 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	☑ C ☐ No ☐ N/A	

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	☑ C ☐ No ☐ N/A	
391	6.4.6.3	All communications on the 4.9G Hz band should be encrypted?	BP	☑ C ☐ No ☐ N/A	
392	6.4.6.3	Authentication, authorization, and accountability should be maintained.	BP	☑ 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	☑ 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	☐ C ☑ No ☐ N/A	However, many do hold certifications

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	☑ 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	☑ C ☐ No ☐ N/A	
Section 14 – Wireless Security			Auditor:		Date: 5/22/2020

Auditor Comments:

It is worthy to note that all of the above requirements are easily executable by Hamilton NG911 based on the customer's need.

Initial risk assessments and the recommendations that come from those assessments will allow Hamilton NG911 make a recommendation based on the clients unique risk landscape.

Hamilton NG911's client security posture will always be evolving and Hamilton has put into place a robust and maliable security strategy that allows security personal to adjust to that ever changing landscape.

Auditor Notes

Auditor Instructions:

HAMILTON APPENDIX 7: PANDEMIC/INFECTIOUS DISEASE PLAN

Pandemic/Infectious Disease Plan

In addition to other components of our business continuity plans, we have had a pandemic response plan in place for the past several years. Our management team actively and routinely reviews and revises our Pandemic/Infectious Disease and Disaster Recovery Plan to make sure that it contains information that is both current and relevant. Some specifics of the plan include:

- Maintain a list of local emergency contacts, ensuring the accuracy of contact information.
- Maintain a sufficient supply of particle masks, antibacterial hand soaps, hand sanitizers, and cleaning supplies.
- Maintain a sufficient supply of water, food and hygiene products if staff were needed to stay in our facilities for a period of time.
- Post flyers containing health tips and safety instructions in visible locations.
- Routine communication with each of our teams and employees regarding health tips and safety instructions.
- Designated a crisis response team responsible for observation, understanding, preparedness and response planning surrounding CDC guidelines and communicating guidelines and recommendations for prevention with all staff.

2020 Covid-19 Pandemic

In response to the current Covid-19 pandemic, we activated our Pandemic/Infectious Disease Plan and refined it to meet current CDC requirements. This unprecedented pandemic situation, resulting in a declaration of a national emergency, also resulted in the activation of our holistic pandemic plan. At Hamilton, our mission has always been to keep people connected, and during times of crisis, that mission becomes even more important. The priority of this plan is to ensure we continue to deliver uninterrupted high-quality services to our customers while also making sure we keep our employees, customers and our communities safe and healthy.

As part of our response plan:

- Our Senior Management and response team meets daily, assessing the situation and ensuring the plan is implemented, and is updated as needed to match current situations.

- We expanded our existing telecommuting policies and procedures company-wide, ensuring that employees have the required equipment, network access and security to work from home. We implemented a phased approach for employees to telecommute, sending employees who were not essential to being inside one of our buildings home first and have tiered plans should we need to have all employees working from home.

- We obtained travel and access letters from the Department of Homeland Security to allow Hamilton employees to travel to work as needed during any curfew or shelter-in-place directive from state or local officials.

- We communicated our plans and the essential nature for some of our employees to be in the building and need to travel to and from work with local/state law enforcement.

- We have restricted access to our buildings to employees and essential vendors.

- For the health and well-being of our employees, we implemented the following in each of our buildings and office locations:
    - Increased hygiene awareness and supplies (handwashing and hand sanitizers, wiping down workstations, etc.).
    - Increased cleaning throughout the center (wiping down surfaces throughout the day, more extensive cleaning routines, misting alcohol spray in workstations, etc.).
    - Adapted attendance and PTO policies to support employees' personal needs, whether that be childcare issues, exposure concerns, personal illness or self-quarantining.
    - Adjusted procedures and processes to improve social distancing and reduce physical contact with common items.

- Communicated information to our employees frequently through an employee intranet; posters and videos; and through text messaging to ensure all employees have access to the information they need.

- In the best interest for those in our local communities as well as our employees, we suspended all travel and in-person outreach activities. Our teams have been working to connect through webinars, online meetings and other online activities while we continue to plan future events.

- We are communicating often with our State Administrators and the FCC to keep them informed about the issues and steps being taken to address issues as they arise. We informed them early on and at regular intervals of our plans and what is happening.

- We have been in regular communication with each of our states so that we can stay informed of state actions and plans and use this information to make decisions appropriate for each location.

- We are listening to our states and working hard to communicate with them in a clear, cooperative way. We appreciate and value regular collaboration during these unparalleled times.

Keeping Our Customers Informed

As part of our continuing effort to keep our customers informed we posted customer notifications on the Hamilton Telecommunications and Hamilton Relay websites and shared the information in e-blasts.

The current situation around COVID-19 continues to evolve even as we prepared our response to this bid. Our preparedness has given us the ability to be proactive, rather than reactive, and to quickly make decisions as situations change. This is key to our ability to ensure essential services. Our number one priority is to always ensure that people and customers who rely on our critical services have uninterrupted, secure and reliable access to them. It is this forward-thinking planning and preparation that makes Hamilton the right choice to provide critical Next Generation 9-1-1 services for Nebraska.

HAMILTON APPENDIX 8: SAMPLE TEST PLAN

(CONFIDENTIAL & PROPRIETARY INFORMATION)

Page intentionally left blank.

To view Sample Test Plan, please see, "**PROPRIETARY INFORMATION**" electronic file.

HAMILTON APPENDIX 9: 2020 TRUST SERVICES CRITERIA (TSC) SELF-ASSESSMENT

Hamilton NG911, Inc
2020 Trust Services Criteria (TSC) Self Assessment
Conducted by Robert Leonard, ISM, Security + Certified

TSC Ref. #	Criteria	Assessment
	CONTROL ENVIRONMENT	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Controls in place
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Controls in place
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Controls in place
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Controls in place
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Controls in place
	COMMUNICATION AND INFORMATION	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Controls in place
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Controls in place
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Controls in place
	RISK ASSESSMENT	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Controls in place
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Controls in place
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Controls in place
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Controls in place
	MONITORING ACTIVITIES	
CC4.1	COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Controls in place
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Controls in place
	CONTROL ACTIVITIES	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls in place
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Controls in place
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Controls in place

	Logical and Physical Access Controls	
CC6.1	*The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.*	Controls in place
CC6.2	*Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*	Controls in place
CC6.3	*The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.*	Controls in place
CC6.4	*The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*	Controls in place
CC6.5	*The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.*	Controls in place
CC6.6	*The entity implements logical access security measures to protect against threats from sources outside its system boundaries.*	Controls in place
CC6.7	*The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.*	Controls in place
CC6.8	*The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.*	Controls in place
	System Operations	
CC7.1	*To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.*	Controls in place
CC7.2	*The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.*	Controls in place
CC7.3	*The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.*	Controls in place
CC7.4	*The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.*	Controls in place
CC7.5	*The entity identifies, develops, and implements activities to recover from identified security incidents.*	Controls in place
	Change Management	
CC8.1	*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*	Controls in place
	Risk Mitigation	
CC9.1	*The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.*	Controls in place
CC9.2	*The entity assesses and manages risks associated with vendors and business partners.*	Controls in place
	ADDITIONAL CRITERIA FOR AVAILABILITY	

A1.1	*The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.*	Controls in place
A1.2	*The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.*	Controls in place
A1.3	*The entity tests recovery plan procedures supporting system recovery to meet its objectives.*	Controls in place
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY	
C1.1	*The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.*	Controls in place
C1.2	*The entity disposes of confidential information to meet the entity's objectives related to confidentiality.*	Controls in place
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY	
PI1.1	*The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.*	Controls in place
PI1.2	*The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.*	Controls in place
PI1.3	*The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.*	Controls in place
PI1.4	*The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.*	Controls in place
PI1.5	*The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.*	Controls in place
	ADDITIONAL CRITERIA FOR PRIVACY	
P1.0	Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy	
P1.1	*The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.*	Controls in place
P2.0	Privacy Criteria Related to Choice and Consent	
P2.1	*The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.*	Controls in place
P3.0	Privacy Criteria Related to Collection	
P3.1	*Personal information is collected consistent with the entity's objectives related to privacy.*	Controls in place
P3.2	*For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.*	Controls in place
P4.0	Privacy Criteria Related to Use, Retention, and Disposal	

P4.1	*The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.*	Controls in place
P4.2	*The entity retains personal information consistent with the entity's objectives related to privacy.*	Controls in place
P4.3	*The entity securely disposes of personal information to meet the entity's objectives related to privacy.*	Controls in place
P5.0	Privacy Criteria Related to Access	
P5.1	*The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.*	Controls in place
P5.2	*The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.*	Controls in place
P6.0	Privacy Criteria Related to Disclosure and Notification	
P6.1	*The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.*	Controls in place
P6.2	*The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.*	Controls in place
P6.3	*The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.*	Controls in place
P6.4	*The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.*	Controls in place
P6.5	*The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.*	Controls in place
P6.6	*The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.*	Controls in place
P6.7	*The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.*	Controls in place
P7.0	Privacy Criteria Related to Quality	
P7.1	*The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.*	Controls in place
P8.0	Privacy Criteria Related to Monitoring and Enforcement	
P8.1	*The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.*	Controls in place

HAMILTON APPENDIX 10: ANGEN NG 9-1-1 REPORT FOR THE REPORTING INTERVAL ENDING JANUARY 6, 2019

<<PROPRIETARY OR CONFIDENTIAL INFORMATION INTENTIONALLY REMOVED>>

HAMILTON APPENDIX 11: NEBRASKA PROJECT PLAN TEMPLATE

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
1	**Project Start**	**458 days**	**Thu 10/1/20**	**Mon 7/4/22**
2	**NGCS**	**458 days**	**Thu 10/1/20**	**Mon 7/4/22**
3	Receive Signed Contract	1 day	Thu 10/1/20	Thu 10/1/20
4	Develop scope of work	1 day	Fri 10/2/20	Fri 10/2/20
5	**Design Phase**	**111 days**	**Fri 10/2/20**	**Fri 3/5/21**
6	**Call Flow questionnaire**	**25 days**	**Fri 10/2/20**	**Thu 11/5/20**
7	Distribute call flow questionnaire to CLIENT on a per site(s) basis	10 days	Fri 10/2/20	Thu 10/15/20
8	Gather and categorize questionnaire results	20 days	Fri 10/9/20	Thu 11/5/20
9	**Site assessment**	**30 days**	**Fri 10/2/20**	**Thu 11/12/20**
10	**Site Survey**	**30 days**	**Fri 10/2/20**	**Thu 11/12/20**
11	**Hosts**	**30 days**	**Fri 10/2/20**	**Thu 11/12/20**
12	Data Center A	30 days	Fri 10/2/20	Thu 11/12/20
13	Data Center B	30 days	Fri 10/2/20	Thu 11/12/20
14	**Transport Requirements**	**10 days**	**Fri 11/6/20**	**Thu 11/19/20**
15	SS7 / Sigtran design	10 days	Fri 11/6/20	Thu 11/19/20
16	Carrier trunking Ingress Network design (T1, DS3, OCx)	10 days	Fri 11/6/20	Thu 11/19/20
17	Ethernet (WAN) Network design	10 days	Fri 11/6/20	Thu 11/19/20
18	Commodity Network design	10 days	Fri 11/6/20	Thu 11/19/20
19	**ESInet Requirements**	**15 days**	**Fri 11/13/20**	**Thu 12/3/20**
20	ESInet design completed	15 days	Fri 11/13/20	Thu 12/3/20
21	Circuit Diagrams	15 days	Fri 11/13/20	Thu 12/3/20
22	ESInet design approved	15 days	Fri 11/13/20	Thu 12/3/20
23	**NG Core Network Requirements**	**81 days**	**Fri 11/13/20**	**Fri 3/5/21**
24	**VM Host**	**35 days**	**Fri 11/13/20**	**Thu 12/31/20**
25	SBC, iBCF, ESRP, eBCF design complete	15 days	Fri 11/13/20	Thu 12/3/20

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
26	Server equipment specifications complete	15 days	Fri 11/20/20	Thu 12/10/20
27	IP Scheme developed for Core network	15 days	Fri 12/11/20	Thu 12/31/20
28	**Routers**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
29	Router network design complete	1 day	Fri 11/20/20	Fri 11/20/20
30	Router equipment specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
31	**Switches (3650s)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
32	Switch network design complete	1 day	Fri 11/20/20	Fri 11/20/20
33	Switch equipment specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
34	**Local Network Gateway (LNG)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
35	LNG network design complete	1 day	Fri 11/20/20	Fri 11/20/20
36	LNG equipment specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
37	**DACs**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
38	DACs design complete	1 day	Fri 11/20/20	Fri 11/20/20
39	DACs specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
40	**Monitoring**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
41	Monitoring design complete	1 day	Fri 11/20/20	Fri 11/20/20
42	Montoring specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
43	**Mevo Server (optional)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
44	Mevo Server design complete	1 day	Fri 11/20/20	Fri 11/20/20
45	Mevo Server specifications complete	5 days	Mon 11/23/20	Fri 11/27/20
46	**NG ALI Servers (Phase 2)**	**30 days**	**Fri 11/20/20**	**Thu 12/31/20**
47	NG ALI Server design complete	20 days	Fri 11/20/20	Thu 12/17/20
48	NG ALI Server specifications complete	10 days	Fri 12/18/20	Thu 12/31/20
49	**Domain Name System (DNS)**	**5 days**	**Fri 11/20/20**	**Thu 11/26/20**

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
50	DNS design complete	5 days	Fri 11/20/20	Thu 11/26/20
51	**NTP Time Synchronization**	**5 days**	**Fri 11/20/20**	**Thu 11/26/20**
52	NTP design complete	5 days	Fri 11/20/20	Thu 11/26/20
53	**Dial Plan Proxy (DPP)**	**35 days**	**Fri 11/20/20**	**Thu 1/7/21**
54	DPP design complete	5 days	Fri 11/20/20	Thu 11/26/20
55	PSTN Telephone Service provided	30 days	Fri 11/27/20	Thu 1/7/21
56	800 Fail-Over Assignment	5 days	Fri 11/20/20	Thu 11/26/20
57	Common Language Functional Elements (CLFE) Assignment	5 days	Mon 3/1/21	Fri 3/5/21
58	Power / UPS design	5 days	Fri 11/13/20	Thu 11/19/20
59	Physical/Spares	30 days	Fri 11/13/20	Thu 12/24/20
60	**RCH Network Requirements**	**60 days**	**Fri 11/13/20**	**Thu 2/4/21**
61	**Texty design (optional)**	**30 days**	**Fri 11/13/20**	**Thu 12/24/20**
62	Determine deployment requirements - OT	30 days	Fri 11/13/20	Thu 12/24/20
63	**ALI (Local pickup)**	**10 days**	**Fri 12/18/20**	**Thu 12/31/20**
64	ALI interface (Perle / Lantronix) design complete	5 days	Fri 12/18/20	Thu 12/24/20
65	ALI equipment specifications complete	5 days	Fri 12/25/20	Thu 12/31/20
66	**Documentation**	**30 days**	**Fri 12/25/20**	**Thu 2/4/21**
67	Physical System Diagram complete	30 days	Fri 12/25/20	Thu 2/4/21
68	Logical System Diagram complete	30 days	Fri 12/25/20	Thu 2/4/21
69	**Development Phase**	**186 days**	**Mon 11/23/20**	**Mon 8/9/21**
70	**ESInet**	**132 days**	**Fri 2/5/21**	**Mon 8/9/21**
71	"Providers" Network Availability (driven by priority sheets)	132 days	Fri 2/5/21	Mon 8/9/21
72	**Host Site Hardware**	**70 days**	**Mon 11/23/20**	**Fri 2/26/21**
73	**Data Center A (New)**	**70 days**	**Mon 11/23/20**	**Fri 2/26/21**
74	**Equipment Order**	**69 days**	**Mon 11/23/20**	**Thu 2/25/21**

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
75	**VM Servers**	**60 days**	**Fri 12/4/20**	**Thu 2/25/21**
76	Purchase order request	16 days	Fri 12/4/20	Fri 12/25/20
77	Order processed	5 days	Mon 12/28/20	Fri 1/1/21
78	Equipment received	30 days	Mon 12/28/20	Fri 2/5/21
79	Stage & Configure	14 days	Mon 2/8/21	Thu 2/25/21
80	**NG ALI Servers**	**41 days**	**Fri 12/18/20**	**Fri 2/12/21**
81	Purchase order request	10 days	Fri 12/18/20	Thu 12/31/20
82	Order processed	5 days	Fri 1/1/21	Thu 1/7/21
83	Equipment received	21 days	Fri 1/8/21	Fri 2/5/21
84	Stage & Configure	5 days	Mon 2/8/21	Fri 2/12/21
85	**Routers (ASR 1001)**	**50 days**	**Mon 11/23/20**	**Fri 1/29/21**
86	Purchase order request	10 days	Mon 11/23/20	Fri 12/4/20
87	Order processed	5 days	Mon 12/7/20	Fri 12/11/20
88	Equipment received	21 days	Mon 12/14/20	Mon 1/11/21
89	Stage & Configure	14 days	Tue 1/12/21	Fri 1/29/21
90	**Switches (3650s)**	**50 days**	**Mon 11/23/20**	**Fri 1/29/21**
91	Purchase order request	10 days	Mon 11/23/20	Fri 12/4/20
92	Order processed	5 days	Mon 12/7/20	Fri 12/11/20
93	Equipment received	21 days	Mon 12/14/20	Mon 1/11/21
94	Stage & Configure	14 days	Tue 1/12/21	Fri 1/29/21
95	**Local Network Gateway (LNG)**	**50 days**	**Mon 11/23/20**	**Fri 1/29/21**
96	Purchase order request	10 days	Mon 11/23/20	Fri 12/4/20
97	Order processed	5 days	Mon 12/7/20	Fri 12/11/20
98	Equipment received	21 days	Mon 12/14/20	Mon 1/11/21
99	Stage & Configure	14 days	Tue 1/12/21	Fri 1/29/21
100	**DACs ordering**	**50 days**	**Mon 11/23/20**	**Fri 1/29/21**
101	Purchase order request	10 days	Mon 11/23/20	Fri 12/4/20
102	Order processed	5 days	Mon 12/7/20	Fri 12/11/20
103	Equipment received	21 days	Mon 12/14/20	Mon 1/11/21
104	Stage & Configure	14 days	Tue 1/12/21	Fri 1/29/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
105	**Monitoring ordering**	**50 days**	**Mon 11/23/20**	**Fri 1/29/21**
106	Purchase order request	10 days	Mon 11/23/20	Fri 12/4/20
107	Order processed	5 days	Mon 12/7/20	Fri 12/11/20
108	Equipment received	21 days	Mon 12/14/20	Mon 1/11/21
109	Stage & Configure	14 days	Tue 1/12/21	Fri 1/29/21
110	Main Contract for Equipment executed	1 day	Fri 2/26/21	Fri 2/26/21
111	**Data Center B (Established)**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
112	**Equipment Order**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
113	**Routers (ASR 1001)**	**59 days**	**Mon 11/23/20**	**Thu 2/11/21**
114	Purchase order request	5 days	Mon 11/23/20	Fri 11/27/20
115	Order processed	10 days	Mon 11/30/20	Fri 12/11/20
116	Equipment received	30 days	Mon 12/14/20	Fri 1/22/21
117	Stage & Configure	14 days	Mon 1/25/21	Thu 2/11/21
118	Main Contract for Equipment executed	1 day	Fri 2/12/21	Fri 2/12/21
119	**Data Center C (Optional)**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
120	**Equipment Order**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
121	**Routers (ASR 1001)**	**59 days**	**Mon 11/23/20**	**Thu 2/11/21**
122	Purchase order request	5 days	Mon 11/23/20	Fri 11/27/20
123	Order processed	10 days	Mon 11/30/20	Fri 12/11/20
124	Equipment received	30 days	Mon 12/14/20	Fri 1/22/21
125	Stage & Configure	14 days	Mon 1/25/21	Thu 2/11/21
126	Main Contract for Equipment executed	1 day	Fri 2/12/21	Fri 2/12/21
127	**Implementation Phase**	**95 days**	**Fri 10/16/20**	**Thu 2/25/21**
128	**Transport**	**95 days**	**Fri 10/16/20**	**Thu 2/25/21**
129	DACs Installation (Data Center A, Data Center B existing)	14 days	Tue 1/12/21	Fri 1/29/21

ID	Task Name	Duration	Start	Finish
130	**LNG Installation (Data Center A, Data Center B existing)**	**19 days**	**Tue 1/12/21**	**Fri 2/5/21**
131	Dialogic 1010 Installation	14 days	Tue 1/12/21	Fri 1/29/21
132	SS7 / Sigtran Installation	5 days	Mon 2/1/21	Fri 2/5/21
133	SS7 / Sigtran Testing	5 days	Mon 2/1/21	Fri 2/5/21
134	Carrier Trunking turned up & tested	51 days	Fri 11/20/20	Fri 1/29/21
135	Router to Router Turned Up & Tested	14 days	Mon 2/8/21	Thu 2/25/21
136	Transfer Codes Confirmed	30 days	Fri 10/16/20	Thu 11/26/20
137	**ESInet**	**201 days**	**Fri 12/4/20**	**Fri 9/10/21**
138	Network Availability	192 days	Fri 12/4/20	Mon 8/30/21
139	Define/configure call logging (NMIS)	14 days	Tue 8/24/21	Fri 9/10/21
140	**Host sites**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
141	**Data Center A**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
142	**NG Core Network**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
143	Router Installation (ASR1001)	14 days	Tue 1/12/21	Fri 1/29/21
144	Switch Installation (3650s)	14 days	Tue 1/12/21	Fri 1/29/21
145	**Install Host Servers**	**14 days**	**Mon 2/1/21**	**Thu 2/18/21**
146	**Production Configurations**	**14 days**	**Mon 2/1/21**	**Thu 2/18/21**
147	ESRP	14 days	Mon 2/1/21	Thu 2/18/21
148	iBCF	14 days	Mon 2/1/21	Thu 2/18/21
149	eBCF	14 days	Mon 2/1/21	Thu 2/18/21
150	XMS	14 days	Mon 2/1/21	Thu 2/18/21
151	Monitoring	14 days	Mon 2/1/21	Thu 2/18/21
152	Admin	14 days	Mon 2/1/21	Thu 2/18/21
153	Logs	14 days	Mon 2/1/21	Thu 2/18/21
154	Backup	14 days	Mon 2/1/21	Thu 2/18/21
155	SRDB	14 days	Mon 2/1/21	Thu 2/18/21
156	DNS	14 days	Mon 2/1/21	Thu 2/18/21
157	NTP	14 days	Mon 2/1/21	Thu 2/18/21
158	PBX	14 days	Mon 2/1/21	Thu 2/18/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
159	ALI/ECRF	14 days	Mon 2/1/21	Thu 2/18/21
160	MEVO (optional)	14 days	Mon 2/1/21	Thu 2/18/21
161	SBC	14 days	Mon 2/1/21	Thu 2/18/21
162	DPP	14 days	Mon 2/1/21	Thu 2/18/21
163	NG ALI Server installation (Phase 1)	14 days	Mon 2/8/21	Thu 2/25/21
164	**Network Management**	**35 days**	**Mon 2/1/21**	**Fri 3/19/21**
165	Remote Access	5 days	Mon 2/1/21	Fri 2/5/21
166	VLAN Assignment	5 days	Mon 2/1/21	Fri 2/5/21
167	Data Center A As-built documentation	30 days	Mon 2/8/21	Fri 3/19/21
168	**Data Center B**	**40 days**	**Mon 1/25/21**	**Fri 3/19/21**
169	**NG Core Network**	**40 days**	**Mon 1/25/21**	**Fri 3/19/21**
170	Router Installation - Existing	5 days	Mon 1/25/21	Fri 1/29/21
171	Switch Installation (3650s) - Existing	5 days	Mon 1/25/21	Fri 1/29/21
172	**Install Host Servers (Existing)**	**14 days**	**Mon 2/1/21**	**Thu 2/18/21**
190	NG ALI Server installation - Existing (Phase 1)	1 day	Mon 2/8/21	Mon 2/8/21
191	**Network Management (Existing)**	**35 days**	**Mon 2/1/21**	**Fri 3/19/21**
195	**Region Conversion**	**397 days**	**Fri 12/25/20**	**Mon 7/4/22**
196	**South Central Region**	**309 days**	**Fri 12/25/20**	**Wed 3/2/22**
197	**WAN Testing**	**15 days**	**Mon 3/22/21**	**Fri 4/9/21**
198	**Pre-ConversionTesting**	**15 days**	**Mon 3/22/21**	**Fri 4/9/21**
209	**Network Conversion Capability Turn-up**	**111 days**	**Fri 12/25/20**	**Fri 5/28/21**
210	Policy Routing Function (PRF)	10 days	Tue 3/23/21	Mon 4/5/21
211	Network Fail-Over	10 days	Tue 3/23/21	Mon 4/5/21
212	VM Fail-Over	10 days	Tue 3/23/21	Mon 4/5/21
213	**Acceptance testing - 1st Functional Acceptance testing**	**39 days**	**Tue 4/6/21**	**Fri 5/28/21**
214	Testing	5 days	Tue 4/6/21	Mon 4/12/21
215	Plan/Criteria/Cases-Scenario's	1 day	Tue 4/13/21	Tue 4/13/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
216	Component testing	1 day	Tue 4/13/21	Tue 4/13/21
217	Functional testing	1 day	Tue 4/13/21	Tue 4/13/21
218	Admin Failover testing	1 day	Tue 4/13/21	Tue 4/13/21
219	Failover testing	1 day	Tue 4/13/21	Tue 4/13/21
220	**Final full operational system test**	**5 days**	**Wed 4/14/21**	**Tue 4/20/21**
221	Testing	5 days	Wed 4/14/21	Tue 4/20/21
222	Plan/Criteria/Cases-Scenario's	1 day	Wed 4/14/21	Wed 4/14/21
223	Component testing	1 day	Thu 4/15/21	Thu 4/15/21
224	Functional testing	1 day	Fri 4/16/21	Fri 4/16/21
225	Failover testing	1 day	Mon 4/19/21	Mon 4/19/21
226	**Final Acceptance testing**	**30 days**	**Mon 4/19/21**	**Fri 5/28/21**
227	Test documentation	30 days	Mon 4/19/21	Fri 5/28/21
228	Test report	30 days	Mon 4/19/21	Fri 5/28/21
229	Final Design Documentation	30 days	Mon 4/19/21	Fri 5/28/21
230	TEXTY testing and turn-up (optional)	90 days	Fri 12/25/20	Thu 4/29/21
231	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
232	NMIS Data Exchange	1 day	Mon 4/19/21	Mon 4/19/21
233	Carrier Notification complete	10 days	Fri 2/5/21	Thu 2/18/21
234	Conversion packets complete	10 days	Fri 2/5/21	Thu 2/18/21
235	Carrier Facilities complete	30 days	Fri 2/19/21	Thu 4/1/21
236	Individual Carrier Calls Complete	90 days	Fri 2/19/21	Thu 6/24/21
237	**Carrier Facilities Oversight**	**30 days**	**Fri 2/19/21**	**Thu 4/1/21**
238	Trunk Order Received	20 days	Fri 2/19/21	Thu 3/18/21
239	Trunks Tested and Turned Up	30 days	Fri 2/19/21	Thu 4/1/21
240	ISUP Connection Order (Point Code to Point Code Connection)	24 days	Fri 2/19/21	Wed 3/24/21
241	Carrier Conversions Scheduled	10 days	Tue 4/20/21	Mon 5/3/21
242	Carrier Conversions complete	30 days	Thu 3/25/21	Wed 5/5/21
243	**Cut Over**	**3 days**	**Tue 5/4/21**	**Thu 5/6/21**

ID	Task Name	Duration	Start	Finish
244	RCHs migrated to VENDOR selective routing (from summary sheet)	1 day	Tue 5/4/21	Tue 5/4/21
245	Cut Over Complete (from summary sheet)	1 day	Thu 5/6/21	Thu 5/6/21
246	**Buffalo County Regional Call Host (RCH)**	**208 days**	**Fri 5/7/21**	**Tue 2/22/22**
247	**RCH Physical Network Configuration**	**188 days**	**Fri 5/7/21**	**Tue 1/25/22**
248	Project Kick Off	1 day	Fri 5/7/21	Fri 5/7/21
249	**Site Survey**	**2 days**	**Mon 5/10/21**	**Tue 5/11/21**
250	RCH Survey and Questionnaire Received	1 day	Mon 5/10/21	Mon 5/10/21
251	Survey Documentation Received	1 day	Tue 5/11/21	Tue 5/11/21
252	Initial RCH design	15 days	Mon 5/10/21	Fri 5/28/21
253	Texty (optional) confirmed	15 days	Mon 5/10/21	Fri 5/28/21
254	Rack assignments	15 days	Mon 5/10/21	Fri 5/28/21
255	LAN assignments	15 days	Mon 5/10/21	Fri 5/28/21
256	WAN assignments	15 days	Mon 5/10/21	Fri 5/28/21
257	**Call Flow Design**	**85 days**	**Mon 5/10/21**	**Fri 9/3/21**
258	Call routing documentation complete	85 days	Mon 5/10/21	Fri 9/3/21
259	Call flow logical diagram complete	85 days	Mon 5/10/21	Fri 9/3/21
260	Initial Design Sign Off	10 days	Tue 5/11/21	Mon 5/24/21
261	**RCH router documentation**	**72 days**	**Mon 9/6/21**	**Tue 12/14/21**
262	Configuration specs	15 days	Mon 9/6/21	Fri 9/24/21
263	Router equipment order	1 day	Mon 9/27/21	Mon 9/27/21
264	Router received	30 days	Tue 9/28/21	Mon 11/8/21
265	Router build and stage	15 days	Tue 11/9/21	Mon 11/29/21
266	Router installation	10 days	Tue 11/30/21	Mon 12/13/21

ID	Task Name	Duration	Start	Finish
267	**Router test and soak**	**1 day**	**Tue 11/30/21**	**Tue 11/30/21**
268	Router monitoring and management initiated	1 day	Tue 11/30/21	Tue 11/30/21
269	Documentation of monitoring and management system	1 day	Tue 11/30/21	Tue 11/30/21
270	Router cut over	1 day	Tue 12/14/21	Tue 12/14/21
271	Redline Design Changes Documented	10 days	Wed 12/1/21	Tue 12/14/21
272	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Mon 5/10/21**	**Fri 6/4/21**
273	Cable estimates	1 day	Mon 5/10/21	Mon 5/10/21
274	Cable design complete	5 days	Mon 5/10/21	Fri 5/14/21
275	Run cable	10 days	Tue 5/11/21	Mon 5/24/21
276	Cable Termination	10 days	Mon 5/17/21	Fri 5/28/21
277	Test LAN WAN	5 days	Tue 5/25/21	Mon 5/31/21
278	Install VoIP Phone	5 days	Mon 5/31/21	Fri 6/4/21
279	Ready for service	0 days	Fri 6/4/21	Fri 6/4/21
280	**Network Readiness Complete**	**126 days**	**Fri 6/4/21**	**Mon 11/29/21**
281	NID installed	0 days	Fri 6/4/21	Fri 6/4/21
282	VLAN Provisioning Complete	0 days	Fri 6/4/21	Fri 6/4/21
283	CPE Equipment Installed	0 days	Fri 6/4/21	Fri 6/4/21
284	**Tertiary network established (Commodity Internet)**	**61 days**	**Mon 9/6/21**	**Mon 11/29/21**
285	Tertiary network services documented	5 days	Mon 9/6/21	Fri 9/10/21
286	Tertiary network services designed	10 days	Mon 9/13/21	Fri 9/24/21
287	Tertiary network services ordered	1 day	Mon 9/27/21	Mon 9/27/21

ID	Task Name	Duration	Start	Finish
288	Tertiary network services installed	30 days	Tue 9/28/21	Mon 11/8/21
289	Tertiary network services tested	15 days	Tue 11/9/21	Mon 11/29/21
290	**Admin/PCAP Server (as required)**	**131 days**	**Fri 5/7/21**	**Fri 11/5/21**
291	Admin/PCAP connections documented	45 days	Mon 9/6/21	Fri 11/5/21
292	Admin/PCAP connections designed and installed, initial test	30 days	Mon 6/7/21	Fri 7/16/21
293	Admin/PCAP SIP turned up and tested, final test	1 day	Fri 5/7/21	Fri 5/7/21
294	**LNG Design (audio codes - as required)**	**51 days**	**Mon 5/10/21**	**Mon 7/19/21**
295	LNG design completed	10 days	Mon 5/10/21	Fri 5/21/21
296	LNG ordered	1 day	Mon 5/24/21	Mon 5/24/21
297	LNG recieved	30 days	Tue 5/25/21	Mon 7/5/21
298	LNG configured, installed, and initial testing	10 days	Tue 7/6/21	Mon 7/19/21
299	**911 MEVO (optional) connections**	**102 days**	**Mon 9/6/21**	**Tue 1/25/22**
300	MEVO connections documented	15 days	Mon 9/6/21	Fri 9/24/21
301	MEVO connections designed and installed	30 days	Wed 12/15/21	Tue 1/25/22
302	MEVO Phone turned up and tested	5 days	Mon 9/27/21	Fri 10/1/21
303	**RCH Readiness Certification**	**205 days**	**Wed 5/12/21**	**Tue 2/22/22**
304	Final Design Documented	5 days	Mon 6/7/21	Fri 6/11/21
305	**Test Plan Completion**	**125 days**	**Tue 5/25/21**	**Mon 11/15/21**
306	**RCH routers**	**125 days**	**Tue 5/25/21**	**Mon 11/15/21**

ID	Task Name	Duration	Start	Finish
307	**WAN validation and failover**	**125 days**	**Tue 5/25/21**	**Mon 11/15/21**
308	Primary	5 days	Tue 5/25/21	Mon 5/31/21
309	Secondary	5 days	Tue 5/25/21	Mon 5/31/21
310	Tertiary	5 days	Tue 11/9/21	Mon 11/15/21
311	**ESRP Software Applications**	**205 days**	**Wed 5/12/21**	**Tue 2/22/22**
312	**ESRP Operational**	**30 days**	**Wed 5/12/21**	**Tue 6/22/21**
313	Policy Routing	30 days	Wed 5/12/21	Tue 6/22/21
314	**Policy Routing Failover**	**5 days**	**Wed 6/23/21**	**Tue 6/29/21**
315	Primary failover	5 days	Wed 6/23/21	Tue 6/29/21
316	Secondary failover	5 days	Wed 6/23/21	Tue 6/29/21
317	Admin failover	5 days	Wed 6/23/21	Tue 6/29/21
318	MEVO (optional) failover	5 days	Wed 6/23/21	Tue 6/29/21
319	**Database operational**	**1 day**	**Wed 6/23/21**	**Wed 6/23/21**
320	SRDB transitional conversion documented	1 day	Wed 6/23/21	Wed 6/23/21
321	**RCH toolkit Application**	**21 days**	**Wed 6/23/21**	**Wed 7/21/21**
322	Tool kit credentials documented	10 days	Wed 6/23/21	Tue 7/6/21
323	Tool kit RCH setup complete	10 days	Wed 7/7/21	Tue 7/20/21
324	Tool kit verified	1 day	Wed 7/21/21	Wed 7/21/21
325	Training	20 days	Wed 1/26/22	Tue 2/22/22
326	**Carrier Network Conversion**	**111 days**	**Tue 7/6/21**	**Tue 12/7/21**
327	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Tue 7/6/21	Mon 7/12/21
328	Phase 1B - Confirm CPE Cutover Date	5 days	Tue 9/14/21	Mon 9/20/21
329	Phase 2 - ESRP Configuration	45 days	Tue 7/13/21	Mon 9/13/21
330	Phase 3A - Carrier Trunks installed	0 days	Mon 9/13/21	Mon 9/13/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
331	**Phase 3B - Carrier conversion**	**61 days**	**Tue 9/14/21**	**Tue 12/7/21**
332	Wireless Conversion	1 day	Tue 9/14/21	Tue 9/14/21
333	Wireline Conversion	60 days	Wed 9/15/21	Tue 12/7/21
334	RCH Closeout Complete	0 days	Tue 2/22/22	Tue 2/22/22
335	**Dawson County RCH**	**208 days**	**Mon 5/17/21**	**Wed 3/2/22**
336	**RCH Physical Network Configuration**	**188 days**	**Mon 5/17/21**	**Wed 2/2/22**
337	Project Kick Off	1 day	Mon 5/17/21	Mon 5/17/21
338	**Site Survey**	**2 days**	**Tue 5/18/21**	**Wed 5/19/21**
339	RCH Survey and Questionnaire Received	1 day	Tue 5/18/21	Tue 5/18/21
340	Survey Documentation Received	1 day	Wed 5/19/21	Wed 5/19/21
341	Initial RCH design	15 days	Tue 5/18/21	Mon 6/7/21
342	Texty (optional) confirmed	15 days	Tue 5/18/21	Mon 6/7/21
343	Rack assignments	15 days	Tue 5/18/21	Mon 6/7/21
344	LAN assignments	15 days	Tue 5/18/21	Mon 6/7/21
345	WAN assignments	15 days	Tue 5/18/21	Mon 6/7/21
346	**Call Flow Design**	**85 days**	**Tue 5/18/21**	**Mon 9/13/21**
347	Call routing documentation complete	85 days	Tue 5/18/21	Mon 9/13/21
348	Call flow logical diagram complete	85 days	Tue 5/18/21	Mon 9/13/21
349	Initial Design Sign Off	10 days	Wed 5/19/21	Tue 6/1/21
350	**RCH router documentation**	**72 days**	**Tue 9/14/21**	**Wed 12/22/21**
351	Configuration specs	15 days	Tue 9/14/21	Mon 10/4/21
352	Router equipment order	1 day	Tue 10/5/21	Tue 10/5/21
353	Router received	30 days	Wed 10/6/21	Tue 11/16/21
354	Router build and stage	15 days	Wed 11/17/21	Tue 12/7/21
355	Router installation	10 days	Wed 12/8/21	Tue 12/21/21
356	**Router test and soak**	**1 day**	**Wed 12/8/21**	**Wed 12/8/21**

ID	Task Name	Duration	Start	Finish
357	Router monitoring and management initiated	1 day	Wed 12/8/21	Wed 12/8/21
358	Documentation of monitoring and management system	1 day	Wed 12/8/21	Wed 12/8/21
359	Router cut over	1 day	Wed 12/22/21	Wed 12/22/21
360	Redline Design Changes Documented	10 days	Thu 12/9/21	Wed 12/22/21
361	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Tue 5/18/21**	**Mon 6/14/21**
362	Cable estimates	1 day	Tue 5/18/21	Tue 5/18/21
363	Cable design complete	5 days	Tue 5/18/21	Mon 5/24/21
364	Run cable	10 days	Wed 5/19/21	Tue 6/1/21
365	Cable Termination	10 days	Tue 5/25/21	Mon 6/7/21
366	Test LAN WAN	5 days	Wed 6/2/21	Tue 6/8/21
367	Install VoIP Phone	5 days	Tue 6/8/21	Mon 6/14/21
368	Ready for service	0 days	Mon 6/14/21	Mon 6/14/21
369	**Network Readiness Complete**	**126 days**	**Mon 6/14/21**	**Tue 12/7/21**
370	NID installed	0 days	Mon 6/14/21	Mon 6/14/21
371	VLAN Provisioning Complete	0 days	Mon 6/14/21	Mon 6/14/21
372	CPE Equipment Installed	0 days	Mon 6/14/21	Mon 6/14/21
373	**Tertiary network established (Commodity Internet)**	**61 days**	**Tue 9/14/21**	**Tue 12/7/21**
374	Tertiary network services documented	5 days	Tue 9/14/21	Mon 9/20/21
375	Tertiary network services designed	10 days	Tue 9/21/21	Mon 10/4/21
376	Tertiary network services ordered	1 day	Tue 10/5/21	Tue 10/5/21

ID	Task Name	Duration	Start	Finish
377	Tertiary network services installed	30 days	Wed 10/6/21	Tue 11/16/21
378	Tertiary network services tested	15 days	Wed 11/17/21	Tue 12/7/21
379	**Admin/PCAP Server (as required)**	**131 days**	**Mon 5/17/21**	**Mon 11/15/21**
380	Admin/PCAP connections documented	45 days	Tue 9/14/21	Mon 11/15/21
381	Admin/PCAP connections designed and installed, initial test	30 days	Tue 6/15/21	Mon 7/26/21
382	Admin/PCAP SIP turned up and tested, final test	1 day	Mon 5/17/21	Mon 5/17/21
383	**LNG Design (audio codes - as required)**	**51 days**	**Tue 5/18/21**	**Tue 7/27/21**
384	LNG design completed	10 days	Tue 5/18/21	Mon 5/31/21
385	LNG ordered	1 day	Tue 6/1/21	Tue 6/1/21
386	LNG recieved	30 days	Wed 6/2/21	Tue 7/13/21
387	LNG configured, installed, and initial testing	10 days	Wed 7/14/21	Tue 7/27/21
388	**911 MEVO (optional) connections**	**102 days**	**Tue 9/14/21**	**Wed 2/2/22**
389	MEVO connections documented	15 days	Tue 9/14/21	Mon 10/4/21
390	MEVO connections designed and installed	30 days	Thu 12/23/21	Wed 2/2/22
391	MEVO Phone turned up and tested	5 days	Tue 10/5/21	Mon 10/11/21
392	**RCH Readiness Certification**	**205 days**	**Thu 5/20/21**	**Wed 3/2/22**
393	Final Design Documented	5 days	Tue 6/15/21	Mon 6/21/21
394	**Test Plan Completion**	**125 days**	**Wed 6/2/21**	**Tue 11/23/21**
395	**RCH routers**	**125 days**	**Wed 6/2/21**	**Tue 11/23/21**

ID	Task Name	Duration	Start	Finish
396	**WAN validation and failover**	**125 days**	**Wed 6/2/21**	**Tue 11/23/21**
397	Primary	5 days	Wed 6/2/21	Tue 6/8/21
398	Secondary	5 days	Wed 6/2/21	Tue 6/8/21
399	Tertiary	5 days	Wed 11/17/21	Tue 11/23/21
400	**ESRP Software Applications**	**205 days**	**Thu 5/20/21**	**Wed 3/2/22**
401	**ESRP Operational**	**30 days**	**Thu 5/20/21**	**Wed 6/30/21**
402	Policy Routing	30 days	Thu 5/20/21	Wed 6/30/21
403	**Policy Routing Failover**	**5 days**	**Thu 7/1/21**	**Wed 7/7/21**
404	Primary failover	5 days	Thu 7/1/21	Wed 7/7/21
405	Secondary failover	5 days	Thu 7/1/21	Wed 7/7/21
406	Admin failover	5 days	Thu 7/1/21	Wed 7/7/21
407	MEVO (optional) failover	5 days	Thu 7/1/21	Wed 7/7/21
408	**Database operational**	**1 day**	**Thu 7/1/21**	**Thu 7/1/21**
409	SRDB transitional conversion documented	1 day	Thu 7/1/21	Thu 7/1/21
410	**RCH toolkit Application**	**21 days**	**Thu 7/1/21**	**Thu 7/29/21**
411	Tool kit credentials documented	10 days	Thu 7/1/21	Wed 7/14/21
412	Tool kit RCH setup complete	10 days	Thu 7/15/21	Wed 7/28/21
413	Tool kit verified	1 day	Thu 7/29/21	Thu 7/29/21
414	Training	20 days	Thu 2/3/22	Wed 3/2/22
415	**Carrier Network Conversion**	**111 days**	**Wed 7/14/21**	**Wed 12/15/21**
416	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Wed 7/14/21	Tue 7/20/21
417	Phase 1B - Confirm CPE Cutover Date	5 days	Wed 9/22/21	Tue 9/28/21
418	Phase 2 - ESRP Configuration	45 days	Wed 7/21/21	Tue 9/21/21
419	Phase 3A - Carrier Trunks installed	0 days	Tue 9/21/21	Tue 9/21/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
420	**Phase 3B - Carrier conversion**	**61 days**	**Wed 9/22/21**	**Wed 12/15/21**
421	Wireless Conversion	1 day	Wed 9/22/21	Wed 9/22/21
422	Wireline Conversion	60 days	Thu 9/23/21	Wed 12/15/21
423	RCH Closeout Complete	0 days	Wed 3/2/22	Wed 3/2/22
424	**South East Region**	**344 days**	**Fri 12/25/20**	**Wed 4/20/22**
425	**WAN Testing**	**15 days**	**Mon 4/12/21**	**Fri 4/30/21**
437	**Network Conversion Capability Turn-up**	**126 days**	**Fri 12/25/20**	**Fri 6/18/21**
459	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
474	**Windstream Data Center (M Street) RCH**	**208 days**	**Fri 6/25/21**	**Tue 4/12/22**
475	**RCH Physical Network Configuration**	**188 days**	**Fri 6/25/21**	**Tue 3/15/22**
476	Project Kick Off	1 day	Fri 6/25/21	Fri 6/25/21
477	**Site Survey**	**2 days**	**Mon 6/28/21**	**Tue 6/29/21**
478	RCH Survey and Questionnaire Received	1 day	Mon 6/28/21	Mon 6/28/21
479	Survey Documentation Received	1 day	Tue 6/29/21	Tue 6/29/21
480	Initial RCH design	15 days	Mon 6/28/21	Fri 7/16/21
481	Texty (optional) confirmed	15 days	Mon 6/28/21	Fri 7/16/21
482	Rack assignments	15 days	Mon 6/28/21	Fri 7/16/21
483	LAN assignments	15 days	Mon 6/28/21	Fri 7/16/21
484	WAN assignments	15 days	Mon 6/28/21	Fri 7/16/21
485	**Call Flow Design**	**85 days**	**Mon 6/28/21**	**Fri 10/22/21**
486	Call routing documentation complete	85 days	Mon 6/28/21	Fri 10/22/21
487	Call flow logical diagram complete	85 days	Mon 6/28/21	Fri 10/22/21
488	Initial Design Sign Off	10 days	Tue 6/29/21	Mon 7/12/21
489	**RCH router documentation**	**72 days**	**Mon 10/25/21**	**Tue 2/1/22**
490	Configuration specs	15 days	Mon 10/25/21	Fri 11/12/21

ID	Task Name	Duration	Start	Finish
491	Router equipment order	1 day	Mon 11/15/21	Mon 11/15/21
492	Router received	30 days	Tue 11/16/21	Mon 12/27/21
493	Router build and stage	15 days	Tue 12/28/21	Mon 1/17/22
494	Router installation	10 days	Tue 1/18/22	Mon 1/31/22
495	**Router test and soak**	**1 day**	**Tue 1/18/22**	**Tue 1/18/22**
496	Router monitoring and management initiated	1 day	Tue 1/18/22	Tue 1/18/22
497	Documentation of monitoring and management system	1 day	Tue 1/18/22	Tue 1/18/22
498	Router cut over	1 day	Tue 2/1/22	Tue 2/1/22
499	Redline Design Changes Documented	10 days	Wed 1/19/22	Tue 2/1/22
500	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Mon 6/28/21**	**Fri 7/23/21**
501	Cable estimates	1 day	Mon 6/28/21	Mon 6/28/21
502	Cable design complete	5 days	Mon 6/28/21	Fri 7/2/21
503	Run cable	10 days	Tue 6/29/21	Mon 7/12/21
504	Cable Termination	10 days	Mon 7/5/21	Fri 7/16/21
505	Test LAN WAN	5 days	Tue 7/13/21	Mon 7/19/21
506	Install VoIP Phone	5 days	Mon 7/19/21	Fri 7/23/21
507	Ready for service	0 days	Fri 7/23/21	Fri 7/23/21
508	**Network Readiness Complete**	**126 days**	**Fri 7/23/21**	**Mon 1/17/22**
509	NID installed	0 days	Fri 7/23/21	Fri 7/23/21
510	VLAN Provisioning Complete	0 days	Fri 7/23/21	Fri 7/23/21
511	CPE Equipment Installed	0 days	Fri 7/23/21	Fri 7/23/21
512	**Tertiary network established (Commodity Internet)**	**61 days**	**Mon 10/25/21**	**Mon 1/17/22**
513	Tertiary network services documented	5 days	Mon 10/25/21	Fri 10/29/21

ID	Task Name	Duration	Start	Finish
514	Tertiary network services designed	10 days	Mon 11/1/21	Fri 11/12/21
515	Tertiary network services ordered	1 day	Mon 11/15/21	Mon 11/15/21
516	Tertiary network services installed	30 days	Tue 11/16/21	Mon 12/27/21
517	Tertiary network services tested	15 days	Tue 12/28/21	Mon 1/17/22
518	**Admin/PCAP Server (as required)**	**131 days**	**Fri 6/25/21**	**Fri 12/24/21**
519	Admin/PCAP connections documented	45 days	Mon 10/25/21	Fri 12/24/21
520	Admin/PCAP connections designed and installed, initial test	30 days	Mon 7/26/21	Fri 9/3/21
521	Admin/PCAP SIP turned up and tested, final test	1 day	Fri 6/25/21	Fri 6/25/21
522	**LNG Design (audio codes - as required)**	**51 days**	**Mon 6/28/21**	**Mon 9/6/21**
523	LNG design completed	10 days	Mon 6/28/21	Fri 7/9/21
524	LNG ordered	1 day	Mon 7/12/21	Mon 7/12/21
525	LNG recieved	30 days	Tue 7/13/21	Mon 8/23/21
526	LNG configured, installed, and initial testing	10 days	Tue 8/24/21	Mon 9/6/21
527	**911 MEVO (optional) connections**	**102 days**	**Mon 10/25/21**	**Tue 3/15/22**
528	MEVO connections documented	15 days	Mon 10/25/21	Fri 11/12/21
529	MEVO connections designed and installed	30 days	Wed 2/2/22	Tue 3/15/22
530	MEVO Phone turned up and tested	5 days	Mon 11/15/21	Fri 11/19/21

ID	Task Name	Duration	Start	Finish
531	**RCH Readiness Certification**	**205 days**	**Wed 6/30/21**	**Tue 4/12/22**
532	Final Design Documented	5 days	Mon 7/26/21	Fri 7/30/21
533	**Test Plan Completion**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
534	**RCH routers**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
535	**WAN validation and failover**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
536	Primary	5 days	Tue 7/13/21	Mon 7/19/21
537	Secondary	5 days	Tue 7/13/21	Mon 7/19/21
538	Tertiary	5 days	Tue 12/28/21	Mon 1/3/22
539	**ESRP Software Applications**	**205 days**	**Wed 6/30/21**	**Tue 4/12/22**
540	**ESRP Operational**	**30 days**	**Wed 6/30/21**	**Tue 8/10/21**
541	Policy Routing	30 days	Wed 6/30/21	Tue 8/10/21
542	**Policy Routing Failover**	**5 days**	**Wed 8/11/21**	**Tue 8/17/21**
543	Primary failover	5 days	Wed 8/11/21	Tue 8/17/21
544	Secondary failover	5 days	Wed 8/11/21	Tue 8/17/21
545	Admin failover	5 days	Wed 8/11/21	Tue 8/17/21
546	MEVO (optional) failover	5 days	Wed 8/11/21	Tue 8/17/21
547	**Database operational**	**1 day**	**Wed 8/11/21**	**Wed 8/11/21**
548	SRDB transitional conversion documented	1 day	Wed 8/11/21	Wed 8/11/21
549	**RCH toolkit Application**	**21 days**	**Wed 8/11/21**	**Wed 9/8/21**
550	Tool kit credentials documented	10 days	Wed 8/11/21	Tue 8/24/21
551	Tool kit RCH setup complete	10 days	Wed 8/25/21	Tue 9/7/21
552	Tool kit verified	1 day	Wed 9/8/21	Wed 9/8/21
553	Training	20 days	Wed 3/16/22	Tue 4/12/22
554	**Carrier Network Conversion**	**111 days**	**Tue 8/24/21**	**Tue 1/25/22**
555	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Tue 8/24/21	Mon 8/30/21

ID	Task Name	Duration	Start	Finish
556	Phase 1B - Confirm CPE Cutover Date	5 days	Tue 11/2/21	Mon 11/8/21
557	Phase 2 - ESRP Configuration	45 days	Tue 8/31/21	Mon 11/1/21
558	Phase 3A - Carrier Trunks installed	0 days	Mon 11/1/21	Mon 11/1/21
559	**Phase 3B - Carrier conversion**	**61 days**	**Tue 11/2/21**	**Tue 1/25/22**
560	Wireless Conversion	1 day	Tue 11/2/21	Tue 11/2/21
561	Wireline Conversion	60 days	Wed 11/3/21	Tue 1/25/22
562	RCH Closeout Complete	0 days	Tue 4/12/22	Tue 4/12/22
563	**Windstream Data Center (27th Street) RCH**	**208 days**	**Mon 7/5/21**	**Wed 4/20/22**
564	**RCH Physical Network Configuration**	**188 days**	**Mon 7/5/21**	**Wed 3/23/22**
565	Project Kick Off	1 day	Mon 7/5/21	Mon 7/5/21
566	**Site Survey**	**2 days**	**Tue 7/6/21**	**Wed 7/7/21**
567	RCH Survey and Questionnaire Received	1 day	Tue 7/6/21	Tue 7/6/21
568	Survey Documentation Received	1 day	Wed 7/7/21	Wed 7/7/21
569	Initial RCH design	15 days	Tue 7/6/21	Mon 7/26/21
570	Texty (optional) confirmed	15 days	Tue 7/6/21	Mon 7/26/21
571	Rack assignments	15 days	Tue 7/6/21	Mon 7/26/21
572	LAN assignments	15 days	Tue 7/6/21	Mon 7/26/21
573	WAN assignments	15 days	Tue 7/6/21	Mon 7/26/21
574	**Call Flow Design**	**85 days**	**Tue 7/6/21**	**Mon 11/1/21**
575	Call routing documentation complete	85 days	Tue 7/6/21	Mon 11/1/21
576	Call flow logical diagram complete	85 days	Tue 7/6/21	Mon 11/1/21
577	Initial Design Sign Off	10 days	Wed 7/7/21	Tue 7/20/21
578	**RCH router documentation**	**72 days**	**Tue 11/2/21**	**Wed 2/9/22**

ID	Task Name	Duration	Start	Finish
579	Configuration specs	15 days	Tue 11/2/21	Mon 11/22/21
580	Router equipment order	1 day	Tue 11/23/21	Tue 11/23/21
581	Router received	30 days	Wed 11/24/21	Tue 1/4/22
582	Router build and stage	15 days	Wed 1/5/22	Tue 1/25/22
583	Router installation	10 days	Wed 1/26/22	Tue 2/8/22
584	**Router test and soak**	**1 day**	**Wed 1/26/22**	**Wed 1/26/22**
585	Router monitoring and management initiated	1 day	Wed 1/26/22	Wed 1/26/22
586	Documentation of monitoring and management system	1 day	Wed 1/26/22	Wed 1/26/22
587	Router cut over	1 day	Wed 2/9/22	Wed 2/9/22
588	Redline Design Changes Documented	10 days	Thu 1/27/22	Wed 2/9/22
589	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Tue 7/6/21**	**Mon 8/2/21**
590	Cable estimates	1 day	Tue 7/6/21	Tue 7/6/21
591	Cable design complete	5 days	Tue 7/6/21	Mon 7/12/21
592	Run cable	10 days	Wed 7/7/21	Tue 7/20/21
593	Cable Termination	10 days	Tue 7/13/21	Mon 7/26/21
594	Test LAN WAN	5 days	Wed 7/21/21	Tue 7/27/21
595	Install VoIP Phone	5 days	Tue 7/27/21	Mon 8/2/21
596	Ready for service	0 days	Mon 8/2/21	Mon 8/2/21
597	**Network Readiness Complete**	**126 days**	**Mon 8/2/21**	**Tue 1/25/22**
598	NID installed	0 days	Mon 8/2/21	Mon 8/2/21
599	VLAN Provisioning Complete	0 days	Mon 8/2/21	Mon 8/2/21
600	CPE Equipment Installed	0 days	Mon 8/2/21	Mon 8/2/21
601	**Tertiary network established (Commodity Internet)**	**61 days**	**Tue 11/2/21**	**Tue 1/25/22**

ID	Task Name	Duration	Start	Finish
602	Tertiary network services documented	5 days	Tue 11/2/21	Mon 11/8/21
603	Tertiary network services designed	10 days	Tue 11/9/21	Mon 11/22/21
604	Tertiary network services ordered	1 day	Tue 11/23/21	Tue 11/23/21
605	Tertiary network services installed	30 days	Wed 11/24/21	Tue 1/4/22
606	Tertiary network services tested	15 days	Wed 1/5/22	Tue 1/25/22
607	**Admin/PCAP Server (as required)**	**131 days**	**Mon 7/5/21**	**Mon 1/3/22**
608	Admin/PCAP connections documented	45 days	Tue 11/2/21	Mon 1/3/22
609	Admin/PCAP connections designed and installed, initial test	30 days	Tue 8/3/21	Mon 9/13/21
610	Admin/PCAP SIP turned up and tested, final test	1 day	Mon 7/5/21	Mon 7/5/21
611	**LNG Design (audio codes - as required)**	**51 days**	**Tue 7/6/21**	**Tue 9/14/21**
612	LNG design completed	10 days	Tue 7/6/21	Mon 7/19/21
613	LNG ordered	1 day	Tue 7/20/21	Tue 7/20/21
614	LNG recieved	30 days	Wed 7/21/21	Tue 8/31/21
615	LNG configured, installed, and initial testing	10 days	Wed 9/1/21	Tue 9/14/21
616	**911 MEVO (optional) connections**	**102 days**	**Tue 11/2/21**	**Wed 3/23/22**
617	MEVO connections documented	15 days	Tue 11/2/21	Mon 11/22/21
618	MEVO connections designed and installed	30 days	Thu 2/10/22	Wed 3/23/22

ID	Task Name	Duration	Start	Finish
619	MEVO Phone turned up and tested	5 days	Tue 11/23/21	Mon 11/29/21
620	**RCH Readiness Certification**	**205 days**	**Thu 7/8/21**	**Wed 4/20/22**
621	Final Design Documented	5 days	Tue 8/3/21	Mon 8/9/21
622	**Test Plan Completion**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
623	**RCH routers**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
624	**WAN validation and failover**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
625	Primary	5 days	Wed 7/21/21	Tue 7/27/21
626	Secondary	5 days	Wed 7/21/21	Tue 7/27/21
627	Tertiary	5 days	Wed 1/5/22	Tue 1/11/22
628	**ESRP Software Applications**	**205 days**	**Thu 7/8/21**	**Wed 4/20/22**
629	**ESRP Operational**	**30 days**	**Thu 7/8/21**	**Wed 8/18/21**
630	Policy Routing	30 days	Thu 7/8/21	Wed 8/18/21
631	**Policy Routing Failover**	**5 days**	**Thu 8/19/21**	**Wed 8/25/21**
632	Primary failover	5 days	Thu 8/19/21	Wed 8/25/21
633	Secondary failover	5 days	Thu 8/19/21	Wed 8/25/21
634	Admin failover	5 days	Thu 8/19/21	Wed 8/25/21
635	MEVO (optional) failover	5 days	Thu 8/19/21	Wed 8/25/21
636	**Database operational**	**1 day**	**Thu 8/19/21**	**Thu 8/19/21**
637	SRDB transitional conversion documented	1 day	Thu 8/19/21	Thu 8/19/21
638	**RCH toolkit Application**	**21 days**	**Thu 8/19/21**	**Thu 9/16/21**
639	Tool kit credentials documented	10 days	Thu 8/19/21	Wed 9/1/21
640	Tool kit RCH setup complete	10 days	Thu 9/2/21	Wed 9/15/21
641	Tool kit verified	1 day	Thu 9/16/21	Thu 9/16/21
642	Training	20 days	Thu 3/24/22	Wed 4/20/22
643	**Carrier Network Conversion**	**111 days**	**Wed 9/1/21**	**Wed 2/2/22**

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
644	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Wed 9/1/21	Tue 9/7/21
645	Phase 1B - Confirm CPE Cutover Date	5 days	Wed 11/10/21	Tue 11/16/21
646	Phase 2 - ESRP Configuration	45 days	Wed 9/8/21	Tue 11/9/21
647	Phase 3A - Carrier Trunks installed	0 days	Tue 11/9/21	Tue 11/9/21
648	**Phase 3B - Carrier conversion**	**61 days**	**Wed 11/10/21**	**Wed 2/2/22**
649	Wireless Conversion	1 day	Wed 11/10/21	Wed 11/10/21
650	Wireline Conversion	60 days	Thu 11/11/21	Wed 2/2/22
651	RCH Closeout Complete	0 days	Wed 4/20/22	Wed 4/20/22
652	**Metro Region**	**344 days**	**Fri 12/25/20**	**Wed 4/20/22**
653	**WAN Testing**	**15 days**	**Mon 5/3/21**	**Fri 5/21/21**
665	**Network Conversion Capability Turn-up**	**141 days**	**Fri 12/25/20**	**Fri 7/9/21**
687	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
702	**Douglas County RCH**	**208 days**	**Fri 6/25/21**	**Tue 4/12/22**
703	**RCH Physical Network Configuration**	**188 days**	**Fri 6/25/21**	**Tue 3/15/22**
704	Project Kick Off	1 day	Fri 6/25/21	Fri 6/25/21
705	**Site Survey**	**2 days**	**Mon 6/28/21**	**Tue 6/29/21**
706	RCH Survey and Questionnaire Received	1 day	Mon 6/28/21	Mon 6/28/21
707	Survey Documentation Received	1 day	Tue 6/29/21	Tue 6/29/21
708	Initial RCH design	15 days	Mon 6/28/21	Fri 7/16/21
709	Texty (optional) confirmed	15 days	Mon 6/28/21	Fri 7/16/21
710	Rack assignments	15 days	Mon 6/28/21	Fri 7/16/21
711	LAN assignments	15 days	Mon 6/28/21	Fri 7/16/21
712	WAN assignments	15 days	Mon 6/28/21	Fri 7/16/21
713	**Call Flow Design**	**85 days**	**Mon 6/28/21**	**Fri 10/22/21**

ID	Task Name	Duration	Start	Finish
714	Call routing documentation complete	85 days	Mon 6/28/21	Fri 10/22/21
715	Call flow logical diagram complete	85 days	Mon 6/28/21	Fri 10/22/21
716	Initial Design Sign Off	10 days	Tue 6/29/21	Mon 7/12/21
717	**RCH router documentation**	**72 days**	**Mon 10/25/21**	**Tue 2/1/22**
718	Configuration specs	15 days	Mon 10/25/21	Fri 11/12/21
719	Router equipment order	1 day	Mon 11/15/21	Mon 11/15/21
720	Router received	30 days	Tue 11/16/21	Mon 12/27/21
721	Router build and stage	15 days	Tue 12/28/21	Mon 1/17/22
722	Router installation	10 days	Tue 1/18/22	Mon 1/31/22
723	**Router test and soak**	**1 day**	**Tue 1/18/22**	**Tue 1/18/22**
724	Router monitoring and management initiated	1 day	Tue 1/18/22	Tue 1/18/22
725	Documentation of monitoring and management system	1 day	Tue 1/18/22	Tue 1/18/22
726	Router cut over	1 day	Tue 2/1/22	Tue 2/1/22
727	Redline Design Changes Documented	10 days	Wed 1/19/22	Tue 2/1/22
728	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Mon 6/28/21**	**Fri 7/23/21**
729	Cable estimates	1 day	Mon 6/28/21	Mon 6/28/21
730	Cable design complete	5 days	Mon 6/28/21	Fri 7/2/21
731	Run cable	10 days	Tue 6/29/21	Mon 7/12/21
732	Cable Termination	10 days	Mon 7/5/21	Fri 7/16/21
733	Test LAN WAN	5 days	Tue 7/13/21	Mon 7/19/21
734	Install VoIP Phone	5 days	Mon 7/19/21	Fri 7/23/21
735	Ready for service	0 days	Fri 7/23/21	Fri 7/23/21
736	**Network Readiness Complete**	**126 days**	**Fri 7/23/21**	**Mon 1/17/22**

ID	Task Name	Duration	Start	Finish
737	NID installed	0 days	Fri 7/23/21	Fri 7/23/21
738	VLAN Provisioning Complete	0 days	Fri 7/23/21	Fri 7/23/21
739	CPE Equipment Installed	0 days	Fri 7/23/21	Fri 7/23/21
740	**Tertiary network established (Commodity Internet)**	**61 days**	**Mon 10/25/21**	**Mon 1/17/22**
741	Tertiary network services documented	5 days	Mon 10/25/21	Fri 10/29/21
742	Tertiary network services designed	10 days	Mon 11/1/21	Fri 11/12/21
743	Tertiary network services ordered	1 day	Mon 11/15/21	Mon 11/15/21
744	Tertiary network services installed	30 days	Tue 11/16/21	Mon 12/27/21
745	Tertiary network services tested	15 days	Tue 12/28/21	Mon 1/17/22
746	**Admin/PCAP Server (as required)**	**131 days**	**Fri 6/25/21**	**Fri 12/24/21**
747	Admin/PCAP connections documented	45 days	Mon 10/25/21	Fri 12/24/21
748	Admin/PCAP connections designed and installed, initial test	30 days	Mon 7/26/21	Fri 9/3/21
749	Admin/PCAP SIP turned up and tested, final test	1 day	Fri 6/25/21	Fri 6/25/21
750	**LNG Design (audio codes - as required)**	**51 days**	**Mon 6/28/21**	**Mon 9/6/21**
751	LNG design completed	10 days	Mon 6/28/21	Fri 7/9/21
752	LNG ordered	1 day	Mon 7/12/21	Mon 7/12/21
753	LNG recieved	30 days	Tue 7/13/21	Mon 8/23/21
754	LNG configured, installed, and initial testing	10 days	Tue 8/24/21	Mon 9/6/21

ID	Task Name	Duration	Start	Finish
755	**911 MEVO (optional) connections**	**102 days**	**Mon 10/25/21**	**Tue 3/15/22**
756	MEVO connections documented	15 days	Mon 10/25/21	Fri 11/12/21
757	MEVO connections designed and installed	30 days	Wed 2/2/22	Tue 3/15/22
758	MEVO Phone turned up and tested	5 days	Mon 11/15/21	Fri 11/19/21
759	**RCH Readiness Certification**	**205 days**	**Wed 6/30/21**	**Tue 4/12/22**
760	Final Design Documented	5 days	Mon 7/26/21	Fri 7/30/21
761	**Test Plan Completion**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
762	**RCH routers**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
763	**WAN validation and failover**	**125 days**	**Tue 7/13/21**	**Mon 1/3/22**
764	Primary	5 days	Tue 7/13/21	Mon 7/19/21
765	Secondary	5 days	Tue 7/13/21	Mon 7/19/21
766	Tertiary	5 days	Tue 12/28/21	Mon 1/3/22
767	**ESRP Software Applications**	**205 days**	**Wed 6/30/21**	**Tue 4/12/22**
768	**ESRP Operational**	**30 days**	**Wed 6/30/21**	**Tue 8/10/21**
769	Policy Routing	30 days	Wed 6/30/21	Tue 8/10/21
770	**Policy Routing Failover**	**5 days**	**Wed 8/11/21**	**Tue 8/17/21**
771	Primary failover	5 days	Wed 8/11/21	Tue 8/17/21
772	Secondary failover	5 days	Wed 8/11/21	Tue 8/17/21
773	Admin failover	5 days	Wed 8/11/21	Tue 8/17/21
774	MEVO (optional) failover	5 days	Wed 8/11/21	Tue 8/17/21
775	**Database operational**	**1 day**	**Wed 8/11/21**	**Wed 8/11/21**
776	SRDB transitional conversion documented	1 day	Wed 8/11/21	Wed 8/11/21
777	**RCH toolkit Application**	**21 days**	**Wed 8/11/21**	**Wed 9/8/21**
778	Tool kit credentials documented	10 days	Wed 8/11/21	Tue 8/24/21
779	Tool kit RCH setup complete	10 days	Wed 8/25/21	Tue 9/7/21

ID	Task Name	Duration	Start	Finish
780	Tool kit verified	1 day	Wed 9/8/21	Wed 9/8/21
781	Training	20 days	Wed 3/16/22	Tue 4/12/22
782	**Carrier Network Conversion**	**111 days**	**Tue 8/24/21**	**Tue 1/25/22**
783	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Tue 8/24/21	Mon 8/30/21
784	Phase 1B - Confirm CPE Cutover Date	5 days	Tue 11/2/21	Mon 11/8/21
785	Phase 2 - ESRP Configuration	45 days	Tue 8/31/21	Mon 11/1/21
786	Phase 3A - Carrier Trunks installed	0 days	Mon 11/1/21	Mon 11/1/21
787	**Phase 3B - Carrier conversion**	**61 days**	**Tue 11/2/21**	**Tue 1/25/22**
788	Wireless Conversion	1 day	Tue 11/2/21	Tue 11/2/21
789	Wireline Conversion	60 days	Wed 11/3/21	Tue 1/25/22
790	RCH Closeout Complete	0 days	Tue 4/12/22	Tue 4/12/22
791	**Pottawattamie County (IA) RCH**	**208 days**	**Mon 7/5/21**	**Wed 4/20/22**
792	**RCH Physical Network Configuration**	**188 days**	**Mon 7/5/21**	**Wed 3/23/22**
793	Project Kick Off	1 day	Mon 7/5/21	Mon 7/5/21
794	**Site Survey**	**2 days**	**Tue 7/6/21**	**Wed 7/7/21**
795	RCH Survey and Questionnaire Received	1 day	Tue 7/6/21	Tue 7/6/21
796	Survey Documentation Received	1 day	Wed 7/7/21	Wed 7/7/21
797	Initial RCH design	15 days	Tue 7/6/21	Mon 7/26/21
798	Texty (optional) confirmed	15 days	Tue 7/6/21	Mon 7/26/21
799	Rack assignments	15 days	Tue 7/6/21	Mon 7/26/21
800	LAN assignments	15 days	Tue 7/6/21	Mon 7/26/21
801	WAN assignments	15 days	Tue 7/6/21	Mon 7/26/21
802	**Call Flow Design**	**85 days**	**Tue 7/6/21**	**Mon 11/1/21**

ID	Task Name	Duration	Start	Finish
803	Call routing documentation complete	85 days	Tue 7/6/21	Mon 11/1/21
804	Call flow logical diagram complete	85 days	Tue 7/6/21	Mon 11/1/21
805	Initial Design Sign Off	10 days	Wed 7/7/21	Tue 7/20/21
806	**RCH router documentation**	**72 days**	**Tue 11/2/21**	**Wed 2/9/22**
807	Configuration specs	15 days	Tue 11/2/21	Mon 11/22/21
808	Router equipment order	1 day	Tue 11/23/21	Tue 11/23/21
809	Router received	30 days	Wed 11/24/21	Tue 1/4/22
810	Router build and stage	15 days	Wed 1/5/22	Tue 1/25/22
811	Router installation	10 days	Wed 1/26/22	Tue 2/8/22
812	**Router test and soak**	**1 day**	**Wed 1/26/22**	**Wed 1/26/22**
813	Router monitoring and management initiated	1 day	Wed 1/26/22	Wed 1/26/22
814	Documentation of monitoring and management system	1 day	Wed 1/26/22	Wed 1/26/22
815	Router cut over	1 day	Wed 2/9/22	Wed 2/9/22
816	Redline Design Changes Documented	10 days	Thu 1/27/22	Wed 2/9/22
817	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Tue 7/6/21**	**Mon 8/2/21**
818	Cable estimates	1 day	Tue 7/6/21	Tue 7/6/21
819	Cable design complete	5 days	Tue 7/6/21	Mon 7/12/21
820	Run cable	10 days	Wed 7/7/21	Tue 7/20/21
821	Cable Termination	10 days	Tue 7/13/21	Mon 7/26/21
822	Test LAN WAN	5 days	Wed 7/21/21	Tue 7/27/21
823	Install VoIP Phone	5 days	Tue 7/27/21	Mon 8/2/21
824	Ready for service	0 days	Mon 8/2/21	Mon 8/2/21
825	**Network Readiness Complete**	**126 days**	**Mon 8/2/21**	**Tue 1/25/22**

ID	Task Name	Duration	Start	Finish
826	NID installed	0 days	Mon 8/2/21	Mon 8/2/21
827	VLAN Provisioning Complete	0 days	Mon 8/2/21	Mon 8/2/21
828	CPE Equipment Installed	0 days	Mon 8/2/21	Mon 8/2/21
829	**Tertiary network established (Commodity Internet)**	**61 days**	**Tue 11/2/21**	**Tue 1/25/22**
830	Tertiary network services documented	5 days	Tue 11/2/21	Mon 11/8/21
831	Tertiary network services designed	10 days	Tue 11/9/21	Mon 11/22/21
832	Tertiary network services ordered	1 day	Tue 11/23/21	Tue 11/23/21
833	Tertiary network services installed	30 days	Wed 11/24/21	Tue 1/4/22
834	Tertiary network services tested	15 days	Wed 1/5/22	Tue 1/25/22
835	**Admin/PCAP Server (as required)**	**131 days**	**Mon 7/5/21**	**Mon 1/3/22**
836	Admin/PCAP connections documented	45 days	Tue 11/2/21	Mon 1/3/22
837	Admin/PCAP connections designed and installed, initial test	30 days	Tue 8/3/21	Mon 9/13/21
838	Admin/PCAP SIP turned up and tested, final test	1 day	Mon 7/5/21	Mon 7/5/21
839	**LNG Design (audio codes - as required)**	**51 days**	**Tue 7/6/21**	**Tue 9/14/21**
840	LNG design completed	10 days	Tue 7/6/21	Mon 7/19/21
841	LNG ordered	1 day	Tue 7/20/21	Tue 7/20/21
842	LNG recieved	30 days	Wed 7/21/21	Tue 8/31/21
843	LNG configured, installed, and initial testing	10 days	Wed 9/1/21	Tue 9/14/21

ID	Task Name	Duration	Start	Finish
844	**911 MEVO (optional) connections**	**102 days**	**Tue 11/2/21**	**Wed 3/23/22**
845	MEVO connections documented	15 days	Tue 11/2/21	Mon 11/22/21
846	MEVO connections designed and installed	30 days	Thu 2/10/22	Wed 3/23/22
847	MEVO Phone turned up and tested	5 days	Tue 11/23/21	Mon 11/29/21
848	**RCH Readiness Certification**	**205 days**	**Thu 7/8/21**	**Wed 4/20/22**
849	Final Design Documented	5 days	Tue 8/3/21	Mon 8/9/21
850	**Test Plan Completion**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
851	**RCH routers**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
852	**WAN validation and failover**	**125 days**	**Wed 7/21/21**	**Tue 1/11/22**
853	Primary	5 days	Wed 7/21/21	Tue 7/27/21
854	Secondary	5 days	Wed 7/21/21	Tue 7/27/21
855	Tertiary	5 days	Wed 1/5/22	Tue 1/11/22
856	**ESRP Software Applications**	**205 days**	**Thu 7/8/21**	**Wed 4/20/22**
857	**ESRP Operational**	**30 days**	**Thu 7/8/21**	**Wed 8/18/21**
858	Policy Routing	30 days	Thu 7/8/21	Wed 8/18/21
859	**Policy Routing Failover**	**5 days**	**Thu 8/19/21**	**Wed 8/25/21**
860	Primary failover	5 days	Thu 8/19/21	Wed 8/25/21
861	Secondary failover	5 days	Thu 8/19/21	Wed 8/25/21
862	Admin failover	5 days	Thu 8/19/21	Wed 8/25/21
863	MEVO (optional) failover	5 days	Thu 8/19/21	Wed 8/25/21
864	**Database operational**	**1 day**	**Thu 8/19/21**	**Thu 8/19/21**
865	SRDB transitional conversion documented	1 day	Thu 8/19/21	Thu 8/19/21
866	**RCH toolkit Application**	**21 days**	**Thu 8/19/21**	**Thu 9/16/21**
867	Tool kit credentials documented	10 days	Thu 8/19/21	Wed 9/1/21
868	Tool kit RCH setup complete	10 days	Thu 9/2/21	Wed 9/15/21

ID	Task Name	Duration	Start	Finish
869	Tool kit verified	1 day	Thu 9/16/21	Thu 9/16/21
870	Training	20 days	Thu 3/24/22	Wed 4/20/22
871	**Carrier Network Conversion**	**111 days**	**Wed 9/1/21**	**Wed 2/2/22**
872	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Wed 9/1/21	Tue 9/7/21
873	Phase 1B - Confirm CPE Cutover Date	5 days	Wed 11/10/21	Tue 11/16/21
874	Phase 2 - ESRP Configuration	45 days	Wed 9/8/21	Tue 11/9/21
875	Phase 3A - Carrier Trunks installed	0 days	Tue 11/9/21	Tue 11/9/21
876	**Phase 3B - Carrier conversion**	**61 days**	**Wed 11/10/21**	**Wed 2/2/22**
877	Wireless Conversion	1 day	Wed 11/10/21	Wed 11/10/21
878	Wireline Conversion	60 days	Thu 11/11/21	Wed 2/2/22
879	RCH Closeout Complete	0 days	Wed 4/20/22	Wed 4/20/22
880	**North Central Region**	**352 days**	**Fri 12/25/20**	**Mon 5/2/22**
881	**WAN Testing**	**15 days**	**Mon 5/24/21**	**Fri 6/11/21**
893	**Network Conversion Capability Turn-up**	**156 days**	**Fri 12/25/20**	**Fri 7/30/21**
915	**OSP Service Conversion**	**108 days**	**Fri 2/5/21**	**Tue 7/6/21**
930	**Boyd/Holt RCH**	**208 days**	**Wed 7/7/21**	**Fri 4/22/22**
931	**RCH Physical Network Configuration**	**188 days**	**Wed 7/7/21**	**Fri 3/25/22**
932	Project Kick Off	1 day	Wed 7/7/21	Wed 7/7/21
933	**Site Survey**	**2 days**	**Thu 7/8/21**	**Fri 7/9/21**
934	RCH Survey and Questionnaire Received	1 day	Thu 7/8/21	Thu 7/8/21
935	Survey Documentation Received	1 day	Fri 7/9/21	Fri 7/9/21
936	Initial RCH design	15 days	Thu 7/8/21	Wed 7/28/21
937	Texty (optional) confirmed	15 days	Thu 7/8/21	Wed 7/28/21
938	Rack assignments	15 days	Thu 7/8/21	Wed 7/28/21

ID	Task Name	Duration	Start	Finish
939	LAN assignments	15 days	Thu 7/8/21	Wed 7/28/21
940	WAN assignments	15 days	Thu 7/8/21	Wed 7/28/21
941	**Call Flow Design**	**85 days**	**Thu 7/8/21**	**Wed 11/3/21**
942	Call routing documentation complete	85 days	Thu 7/8/21	Wed 11/3/21
943	Call flow logical diagram complete	85 days	Thu 7/8/21	Wed 11/3/21
944	Initial Design Sign Off	10 days	Fri 7/9/21	Thu 7/22/21
945	**RCH router documentation**	**72 days**	**Thu 11/4/21**	**Fri 2/11/22**
946	Configuration specs	15 days	Thu 11/4/21	Wed 11/24/21
947	Router equipment order	1 day	Thu 11/25/21	Thu 11/25/21
948	Router received	30 days	Fri 11/26/21	Thu 1/6/22
949	Router build and stage	15 days	Fri 1/7/22	Thu 1/27/22
950	Router installation	10 days	Fri 1/28/22	Thu 2/10/22
951	**Router test and soak**	**1 day**	**Fri 1/28/22**	**Fri 1/28/22**
952	Router monitoring and management initiated	1 day	Fri 1/28/22	Fri 1/28/22
953	Documentation of monitoring and management system	1 day	Fri 1/28/22	Fri 1/28/22
954	Router cut over	1 day	Fri 2/11/22	Fri 2/11/22
955	Redline Design Changes Documented	10 days	Mon 1/31/22	Fri 2/11/22
956	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Thu 7/8/21**	**Wed 8/4/21**
957	Cable estimates	1 day	Thu 7/8/21	Thu 7/8/21
958	Cable design complete	5 days	Thu 7/8/21	Wed 7/14/21
959	Run cable	10 days	Fri 7/9/21	Thu 7/22/21
960	Cable Termination	10 days	Thu 7/15/21	Wed 7/28/21
961	Test LAN WAN	5 days	Fri 7/23/21	Thu 7/29/21

ID	Task Name	Duration	Start	Finish
962	Install VoIP Phone	5 days	Thu 7/29/21	Wed 8/4/21
963	Ready for service	0 days	Wed 8/4/21	Wed 8/4/21
964	**Network Readiness Complete**	**126 days**	**Wed 8/4/21**	**Thu 1/27/22**
965	NID installed	0 days	Wed 8/4/21	Wed 8/4/21
966	VLAN Provisioning Complete	0 days	Wed 8/4/21	Wed 8/4/21
967	CPE Equipment Installed	0 days	Wed 8/4/21	Wed 8/4/21
968	**Tertiary network established (Commodity Internet)**	**61 days**	**Thu 11/4/21**	**Thu 1/27/22**
969	Tertiary network services documented	5 days	Thu 11/4/21	Wed 11/10/21
970	Tertiary network services designed	10 days	Thu 11/11/21	Wed 11/24/21
971	Tertiary network services ordered	1 day	Thu 11/25/21	Thu 11/25/21
972	Tertiary network services installed	30 days	Fri 11/26/21	Thu 1/6/22
973	Tertiary network services tested	15 days	Fri 1/7/22	Thu 1/27/22
974	**Admin/PCAP Server (as required)**	**131 days**	**Wed 7/7/21**	**Wed 1/5/22**
975	Admin/PCAP connections documented	45 days	Thu 11/4/21	Wed 1/5/22
976	Admin/PCAP connections designed and installed, initial test	30 days	Thu 8/5/21	Wed 9/15/21
977	Admin/PCAP SIP turned up and tested, final test	1 day	Wed 7/7/21	Wed 7/7/21
978	**LNG Design (audio codes - as required)**	**51 days**	**Thu 7/8/21**	**Thu 9/16/21**
979	LNG design completed	10 days	Thu 7/8/21	Wed 7/21/21
980	LNG ordered	1 day	Thu 7/22/21	Thu 7/22/21

ID	Task Name	Duration	Start	Finish
981	LNG recieved	30 days	Fri 7/23/21	Thu 9/2/21
982	LNG configured, installed, and initial testing	10 days	Fri 9/3/21	Thu 9/16/21
983	**911 MEVO (optional) connections**	**102 days**	**Thu 11/4/21**	**Fri 3/25/22**
984	MEVO connections documented	15 days	Thu 11/4/21	Wed 11/24/21
985	MEVO connections designed and installed	30 days	Mon 2/14/22	Fri 3/25/22
986	MEVO Phone turned up and tested	5 days	Thu 11/25/21	Wed 12/1/21
987	**RCH Readiness Certification**	**205 days**	**Mon 7/12/21**	**Fri 4/22/22**
988	Final Design Documented	5 days	Thu 8/5/21	Wed 8/11/21
989	**Test Plan Completion**	**125 days**	**Fri 7/23/21**	**Thu 1/13/22**
990	**RCH routers**	**125 days**	**Fri 7/23/21**	**Thu 1/13/22**
991	**WAN validation and failover**	**125 days**	**Fri 7/23/21**	**Thu 1/13/22**
992	Primary	5 days	Fri 7/23/21	Thu 7/29/21
993	Secondary	5 days	Fri 7/23/21	Thu 7/29/21
994	Tertiary	5 days	Fri 1/7/22	Thu 1/13/22
995	**ESRP Software Applications**	**205 days**	**Mon 7/12/21**	**Fri 4/22/22**
996	**ESRP Operational**	**30 days**	**Mon 7/12/21**	**Fri 8/20/21**
997	Policy Routing	30 days	Mon 7/12/21	Fri 8/20/21
998	**Policy Routing Failover**	**5 days**	**Mon 8/23/21**	**Fri 8/27/21**
999	Primary failover	5 days	Mon 8/23/21	Fri 8/27/21
1000	Secondary failover	5 days	Mon 8/23/21	Fri 8/27/21
1001	Admin failover	5 days	Mon 8/23/21	Fri 8/27/21
1002	MEVO (optional) failover	5 days	Mon 8/23/21	Fri 8/27/21
1003	**Database operational**	**1 day**	**Mon 8/23/21**	**Mon 8/23/21**
1004	SRDB transitional conversion documented	1 day	Mon 8/23/21	Mon 8/23/21
1005	**RCH toolkit Application**	**21 days**	**Mon 8/23/21**	**Mon 9/20/21**

ID	Task Name	Duration	Start	Finish
1006	Tool kit credentials documented	10 days	Mon 8/23/21	Fri 9/3/21
1007	Tool kit RCH setup complete	10 days	Mon 9/6/21	Fri 9/17/21
1008	Tool kit verified	1 day	Mon 9/20/21	Mon 9/20/21
1009	Training	20 days	Mon 3/28/22	Fri 4/22/22
1010	**Carrier Network Conversion**	**111 days**	**Fri 9/3/21**	**Fri 2/4/22**
1011	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Fri 9/3/21	Thu 9/9/21
1012	Phase 1B - Confirm CPE Cutover Date	5 days	Fri 11/12/21	Thu 11/18/21
1013	Phase 2 - ESRP Configuration	45 days	Fri 9/10/21	Thu 11/11/21
1014	Phase 3A - Carrier Trunks installed	0 days	Thu 11/11/21	Thu 11/11/21
1015	**Phase 3B - Carrier conversion**	**61 days**	**Fri 11/12/21**	**Fri 2/4/22**
1016	Wireless Conversion	1 day	Fri 11/12/21	Fri 11/12/21
1017	Wireline Conversion	60 days	Mon 11/15/21	Fri 2/4/22
1018	RCH Closeout Complete	0 days	Fri 4/22/22	Fri 4/22/22
1019	**Cherry County RCH**	**208 days**	**Thu 7/15/21**	**Mon 5/2/22**
1020	**RCH Physical Network Configuration**	**188 days**	**Thu 7/15/21**	**Mon 4/4/22**
1021	Project Kick Off	1 day	Thu 7/15/21	Thu 7/15/21
1022	**Site Survey**	**2 days**	**Fri 7/16/21**	**Mon 7/19/21**
1023	RCH Survey and Questionnaire Received	1 day	Fri 7/16/21	Fri 7/16/21
1024	Survey Documentation Received	1 day	Mon 7/19/21	Mon 7/19/21
1025	Initial RCH design	15 days	Fri 7/16/21	Thu 8/5/21
1026	Texty (optional) confirmed	15 days	Fri 7/16/21	Thu 8/5/21
1027	Rack assignments	15 days	Fri 7/16/21	Thu 8/5/21
1028	LAN assignments	15 days	Fri 7/16/21	Thu 8/5/21

ID	Task Name	Duration	Start	Finish
1029	WAN assignments	15 days	Fri 7/16/21	Thu 8/5/21
1030	**Call Flow Design**	**85 days**	**Fri 7/16/21**	**Thu 11/11/21**
1031	Call routing documentation complete	85 days	Fri 7/16/21	Thu 11/11/21
1032	Call flow logical diagram complete	85 days	Fri 7/16/21	Thu 11/11/21
1033	Initial Design Sign Off	10 days	Mon 7/19/21	Fri 7/30/21
1034	**RCH router documentation**	**72 days**	**Fri 11/12/21**	**Mon 2/21/22**
1035	Configuration specs	15 days	Fri 11/12/21	Thu 12/2/21
1036	Router equipment order	1 day	Fri 12/3/21	Fri 12/3/21
1037	Router received	30 days	Mon 12/6/21	Fri 1/14/22
1038	Router build and stage	15 days	Mon 1/17/22	Fri 2/4/22
1039	Router installation	10 days	Mon 2/7/22	Fri 2/18/22
1040	**Router test and soak**	**1 day**	**Mon 2/7/22**	**Mon 2/7/22**
1041	Router monitoring and management initiated	1 day	Mon 2/7/22	Mon 2/7/22
1042	Documentation of monitoring and management system	1 day	Mon 2/7/22	Mon 2/7/22
1043	Router cut over	1 day	Mon 2/21/22	Mon 2/21/22
1044	Redline Design Changes Documented	10 days	Tue 2/8/22	Mon 2/21/22
1045	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Fri 7/16/21**	**Thu 8/12/21**
1046	Cable estimates	1 day	Fri 7/16/21	Fri 7/16/21
1047	Cable design complete	5 days	Fri 7/16/21	Thu 7/22/21
1048	Run cable	10 days	Mon 7/19/21	Fri 7/30/21
1049	Cable Termination	10 days	Fri 7/23/21	Thu 8/5/21
1050	Test LAN WAN	5 days	Mon 8/2/21	Fri 8/6/21
1051	Install VoIP Phone	5 days	Fri 8/6/21	Thu 8/12/21

ID	Task Name	Duration	Start	Finish
1052	Ready for service	0 days	Thu 8/12/21	Thu 8/12/21
1053	**Network Readiness Complete**	**126 days**	**Thu 8/12/21**	**Fri 2/4/22**
1054	NID installed	0 days	Thu 8/12/21	Thu 8/12/21
1055	VLAN Provisioning Complete	0 days	Thu 8/12/21	Thu 8/12/21
1056	CPE Equipment Installed	0 days	Thu 8/12/21	Thu 8/12/21
1057	**Tertiary network established (Commodity Internet)**	**61 days**	**Fri 11/12/21**	**Fri 2/4/22**
1058	Tertiary network services documented	5 days	Fri 11/12/21	Thu 11/18/21
1059	Tertiary network services designed	10 days	Fri 11/19/21	Thu 12/2/21
1060	Tertiary network services ordered	1 day	Fri 12/3/21	Fri 12/3/21
1061	Tertiary network services installed	30 days	Mon 12/6/21	Fri 1/14/22
1062	Tertiary network services tested	15 days	Mon 1/17/22	Fri 2/4/22
1063	**Admin/PCAP Server (as required)**	**131 days**	**Thu 7/15/21**	**Thu 1/13/22**
1064	Admin/PCAP connections documented	45 days	Fri 11/12/21	Thu 1/13/22
1065	Admin/PCAP connections designed and installed, initial test	30 days	Fri 8/13/21	Thu 9/23/21
1066	Admin/PCAP SIP turned up and tested, final test	1 day	Thu 7/15/21	Thu 7/15/21
1067	**LNG Design (audio codes - as required)**	**51 days**	**Fri 7/16/21**	**Fri 9/24/21**
1068	LNG design completed	10 days	Fri 7/16/21	Thu 7/29/21
1069	LNG ordered	1 day	Fri 7/30/21	Fri 7/30/21
1070	LNG recieved	30 days	Mon 8/2/21	Fri 9/10/21

ID	Task Name	Duration	Start	Finish
1071	LNG configured, installed, and initial testing	10 days	Mon 9/13/21	Fri 9/24/21
1072	**911 MEVO (optional) connections**	**102 days**	**Fri 11/12/21**	**Mon 4/4/22**
1073	MEVO connections documented	15 days	Fri 11/12/21	Thu 12/2/21
1074	MEVO connections designed and installed	30 days	Tue 2/22/22	Mon 4/4/22
1075	MEVO Phone turned up and tested	5 days	Fri 12/3/21	Thu 12/9/21
1076	**RCH Readiness Certification**	**205 days**	**Tue 7/20/21**	**Mon 5/2/22**
1077	Final Design Documented	5 days	Fri 8/13/21	Thu 8/19/21
1078	**Test Plan Completion**	**125 days**	**Mon 8/2/21**	**Fri 1/21/22**
1079	**RCH routers**	**125 days**	**Mon 8/2/21**	**Fri 1/21/22**
1080	**WAN validation and failover**	**125 days**	**Mon 8/2/21**	**Fri 1/21/22**
1081	Primary	5 days	Mon 8/2/21	Fri 8/6/21
1082	Secondary	5 days	Mon 8/2/21	Fri 8/6/21
1083	Tertiary	5 days	Mon 1/17/22	Fri 1/21/22
1084	**ESRP Software Applications**	**205 days**	**Tue 7/20/21**	**Mon 5/2/22**
1085	**ESRP Operational**	**30 days**	**Tue 7/20/21**	**Mon 8/30/21**
1086	Policy Routing	30 days	Tue 7/20/21	Mon 8/30/21
1087	**Policy Routing Failover**	**5 days**	**Tue 8/31/21**	**Mon 9/6/21**
1088	Primary failover	5 days	Tue 8/31/21	Mon 9/6/21
1089	Secondary failover	5 days	Tue 8/31/21	Mon 9/6/21
1090	Admin failover	5 days	Tue 8/31/21	Mon 9/6/21
1091	MEVO (optional) failover	5 days	Tue 8/31/21	Mon 9/6/21
1092	**Database operational**	**1 day**	**Tue 8/31/21**	**Tue 8/31/21**
1093	SRDB transitional conversion documented	1 day	Tue 8/31/21	Tue 8/31/21
1094	**RCH toolkit Application**	**21 days**	**Tue 8/31/21**	**Tue 9/28/21**

ID	Task Name	Duration	Start	Finish
1095	Tool kit credentials documented	10 days	Tue 8/31/21	Mon 9/13/21
1096	Tool kit RCH setup complete	10 days	Tue 9/14/21	Mon 9/27/21
1097	Tool kit verified	1 day	Tue 9/28/21	Tue 9/28/21
1098	Training	20 days	Tue 4/5/22	Mon 5/2/22
1099	**Carrier Network Conversion**	**111 days**	**Mon 9/13/21**	**Mon 2/14/22**
1100	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Mon 9/13/21	Fri 9/17/21
1101	Phase 1B - Confirm CPE Cutover Date	5 days	Mon 11/22/21	Fri 11/26/21
1102	Phase 2 - ESRP Configuration	45 days	Mon 9/20/21	Fri 11/19/21
1103	Phase 3A - Carrier Trunks installed	0 days	Fri 11/19/21	Fri 11/19/21
1104	**Phase 3B - Carrier conversion**	**61 days**	**Mon 11/22/21**	**Mon 2/14/22**
1105	Wireless Conversion	1 day	Mon 11/22/21	Mon 11/22/21
1106	Wireline Conversion	60 days	Tue 11/23/21	Mon 2/14/22
1107	RCH Closeout Complete	0 days	Mon 5/2/22	Mon 5/2/22
1108	**East Central Region**	**367 days**	**Fri 12/25/20**	**Mon 5/23/22**
1109	**WAN Testing**	**15 days**	**Mon 6/14/21**	**Fri 7/2/21**
1121	**Network Conversion Capability Turn-up**	**171 days**	**Fri 12/25/20**	**Fri 8/20/21**
1143	**OSP Service Conversion**	**123 days**	**Fri 2/5/21**	**Tue 7/27/21**
1158	**City of Columbus RCH**	**208 days**	**Wed 7/28/21**	**Fri 5/13/22**
1159	**RCH Physical Network Configuration**	**188 days**	**Wed 7/28/21**	**Fri 4/15/22**
1160	Project Kick Off	1 day	Wed 7/28/21	Wed 7/28/21
1161	**Site Survey**	**2 days**	**Thu 7/29/21**	**Fri 7/30/21**
1162	RCH Survey and Questionnaire Received	1 day	Thu 7/29/21	Thu 7/29/21
1163	Survey Documentation Received	1 day	Fri 7/30/21	Fri 7/30/21

ID	Task Name	Duration	Start	Finish
1164	Initial RCH design	15 days	Thu 7/29/21	Wed 8/18/21
1165	Texty (optional) confirmed	15 days	Thu 7/29/21	Wed 8/18/21
1166	Rack assignments	15 days	Thu 7/29/21	Wed 8/18/21
1167	LAN assignments	15 days	Thu 7/29/21	Wed 8/18/21
1168	WAN assignments	15 days	Thu 7/29/21	Wed 8/18/21
1169	**Call Flow Design**	**85 days**	**Thu 7/29/21**	**Wed 11/24/21**
1170	Call routing documentation complete	85 days	Thu 7/29/21	Wed 11/24/21
1171	Call flow logical diagram complete	85 days	Thu 7/29/21	Wed 11/24/21
1172	Initial Design Sign Off	10 days	Fri 7/30/21	Thu 8/12/21
1173	**RCH router documentation**	**72 days**	**Thu 11/25/21**	**Fri 3/4/22**
1174	Configuration specs	15 days	Thu 11/25/21	Wed 12/15/21
1175	Router equipment order	1 day	Thu 12/16/21	Thu 12/16/21
1176	Router received	30 days	Fri 12/17/21	Thu 1/27/22
1177	Router build and stage	15 days	Fri 1/28/22	Thu 2/17/22
1178	Router installation	10 days	Fri 2/18/22	Thu 3/3/22
1179	**Router test and soak**	**1 day**	**Fri 2/18/22**	**Fri 2/18/22**
1180	Router monitoring and management initiated	1 day	Fri 2/18/22	Fri 2/18/22
1181	Documentation of monitoring and management system	1 day	Fri 2/18/22	Fri 2/18/22
1182	Router cut over	1 day	Fri 3/4/22	Fri 3/4/22
1183	Redline Design Changes Documented	10 days	Mon 2/21/22	Fri 3/4/22
1184	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Thu 7/29/21**	**Wed 8/25/21**
1185	Cable estimates	1 day	Thu 7/29/21	Thu 7/29/21
1186	Cable design complete	5 days	Thu 7/29/21	Wed 8/4/21

ID	Task Name	Duration	Start	Finish
1187	Run cable	10 days	Fri 7/30/21	Thu 8/12/21
1188	Cable Termination	10 days	Thu 8/5/21	Wed 8/18/21
1189	Test LAN WAN	5 days	Fri 8/13/21	Thu 8/19/21
1190	Install VoIP Phone	5 days	Thu 8/19/21	Wed 8/25/21
1191	Ready for service	0 days	Wed 8/25/21	Wed 8/25/21
1192	**Network Readiness Complete**	**126 days**	**Wed 8/25/21**	**Thu 2/17/22**
1193	NID installed	0 days	Wed 8/25/21	Wed 8/25/21
1194	VLAN Provisioning Complete	0 days	Wed 8/25/21	Wed 8/25/21
1195	CPE Equipment Installed	0 days	Wed 8/25/21	Wed 8/25/21
1196	**Tertiary network established (Commodity Internet)**	**61 days**	**Thu 11/25/21**	**Thu 2/17/22**
1197	Tertiary network services documented	5 days	Thu 11/25/21	Wed 12/1/21
1198	Tertiary network services designed	10 days	Thu 12/2/21	Wed 12/15/21
1199	Tertiary network services ordered	1 day	Thu 12/16/21	Thu 12/16/21
1200	Tertiary network services installed	30 days	Fri 12/17/21	Thu 1/27/22
1201	Tertiary network services tested	15 days	Fri 1/28/22	Thu 2/17/22
1202	**Admin/PCAP Server (as required)**	**131 days**	**Wed 7/28/21**	**Wed 1/26/22**
1203	Admin/PCAP connections documented	45 days	Thu 11/25/21	Wed 1/26/22
1204	Admin/PCAP connections designed and installed, initial test	30 days	Thu 8/26/21	Wed 10/6/21
1205	Admin/PCAP SIP turned up and tested, final test	1 day	Wed 7/28/21	Wed 7/28/21

ID	Task Name	Duration	Start	Finish
1206	**LNG Design (audio codes - as required)**	**51 days**	**Thu 7/29/21**	**Thu 10/7/21**
1207	LNG design completed	10 days	Thu 7/29/21	Wed 8/11/21
1208	LNG ordered	1 day	Thu 8/12/21	Thu 8/12/21
1209	LNG recieved	30 days	Fri 8/13/21	Thu 9/23/21
1210	LNG configured, installed, and initial testing	10 days	Fri 9/24/21	Thu 10/7/21
1211	**911 MEVO (optional) connections**	**102 days**	**Thu 11/25/21**	**Fri 4/15/22**
1212	MEVO connections documented	15 days	Thu 11/25/21	Wed 12/15/21
1213	MEVO connections designed and installed	30 days	Mon 3/7/22	Fri 4/15/22
1214	MEVO Phone turned up and tested	5 days	Thu 12/16/21	Wed 12/22/21
1215	**RCH Readiness Certification**	**205 days**	**Mon 8/2/21**	**Fri 5/13/22**
1216	Final Design Documented	5 days	Thu 8/26/21	Wed 9/1/21
1217	**Test Plan Completion**	**125 days**	**Fri 8/13/21**	**Thu 2/3/22**
1218	**RCH routers**	**125 days**	**Fri 8/13/21**	**Thu 2/3/22**
1219	**WAN validation and failover**	**125 days**	**Fri 8/13/21**	**Thu 2/3/22**
1220	Primary	5 days	Fri 8/13/21	Thu 8/19/21
1221	Secondary	5 days	Fri 8/13/21	Thu 8/19/21
1222	Tertiary	5 days	Fri 1/28/22	Thu 2/3/22
1223	**ESRP Software Applications**	**205 days**	**Mon 8/2/21**	**Fri 5/13/22**
1224	**ESRP Operational**	**30 days**	**Mon 8/2/21**	**Fri 9/10/21**
1225	Policy Routing	30 days	Mon 8/2/21	Fri 9/10/21
1226	**Policy Routing Failover**	**5 days**	**Mon 9/13/21**	**Fri 9/17/21**
1227	Primary failover	5 days	Mon 9/13/21	Fri 9/17/21
1228	Secondary failover	5 days	Mon 9/13/21	Fri 9/17/21
1229	Admin failover	5 days	Mon 9/13/21	Fri 9/17/21
1230	MEVO (optional) failover	5 days	Mon 9/13/21	Fri 9/17/21

ID	Task Name	Duration	Start	Finish
1231	**Database operational**	**1 day**	**Mon 9/13/21**	**Mon 9/13/21**
1232	SRDB transitional conversion documented	1 day	Mon 9/13/21	Mon 9/13/21
1233	**RCH toolkit Application**	**21 days**	**Mon 9/13/21**	**Mon 10/11/21**
1234	Tool kit credentials documented	10 days	Mon 9/13/21	Fri 9/24/21
1235	Tool kit RCH setup complete	10 days	Mon 9/27/21	Fri 10/8/21
1236	Tool kit verified	1 day	Mon 10/11/21	Mon 10/11/21
1237	Training	20 days	Mon 4/18/22	Fri 5/13/22
1238	**Carrier Network Conversion**	**111 days**	**Fri 9/24/21**	**Fri 2/25/22**
1239	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Fri 9/24/21	Thu 9/30/21
1240	Phase 1B - Confirm CPE Cutover Date	5 days	Fri 12/3/21	Thu 12/9/21
1241	Phase 2 - ESRP Configuration	45 days	Fri 10/1/21	Thu 12/2/21
1242	Phase 3A - Carrier Trunks installed	0 days	Thu 12/2/21	Thu 12/2/21
1243	**Phase 3B - Carrier conversion**	**61 days**	**Fri 12/3/21**	**Fri 2/25/22**
1244	Wireless Conversion	1 day	Fri 12/3/21	Fri 12/3/21
1245	Wireline Conversion	60 days	Mon 12/6/21	Fri 2/25/22
1246	RCH Closeout Complete	0 days	Fri 5/13/22	Fri 5/13/22
1247	**Saunders County RCH**	**208 days**	**Thu 8/5/21**	**Mon 5/23/22**
1248	**RCH Physical Network Configuration**	**188 days**	**Thu 8/5/21**	**Mon 4/25/22**
1249	Project Kick Off	1 day	Thu 8/5/21	Thu 8/5/21
1250	**Site Survey**	**2 days**	**Fri 8/6/21**	**Mon 8/9/21**
1251	RCH Survey and Questionnaire Received	1 day	Fri 8/6/21	Fri 8/6/21
1252	Survey Documentation Received	1 day	Mon 8/9/21	Mon 8/9/21

ID	Task Name	Duration	Start	Finish
1253	Initial RCH design	15 days	Fri 8/6/21	Thu 8/26/21
1254	Texty (optional) confirmed	15 days	Fri 8/6/21	Thu 8/26/21
1255	Rack assignments	15 days	Fri 8/6/21	Thu 8/26/21
1256	LAN assignments	15 days	Fri 8/6/21	Thu 8/26/21
1257	WAN assignments	15 days	Fri 8/6/21	Thu 8/26/21
1258	**Call Flow Design**	**85 days**	**Fri 8/6/21**	**Thu 12/2/21**
1259	Call routing documentation complete	85 days	Fri 8/6/21	Thu 12/2/21
1260	Call flow logical diagram complete	85 days	Fri 8/6/21	Thu 12/2/21
1261	Initial Design Sign Off	10 days	Mon 8/9/21	Fri 8/20/21
1262	**RCH router documentation**	**72 days**	**Fri 12/3/21**	**Mon 3/14/22**
1263	Configuration specs	15 days	Fri 12/3/21	Thu 12/23/21
1264	Router equipment order	1 day	Fri 12/24/21	Fri 12/24/21
1265	Router received	30 days	Mon 12/27/21	Fri 2/4/22
1266	Router build and stage	15 days	Mon 2/7/22	Fri 2/25/22
1267	Router installation	10 days	Mon 2/28/22	Fri 3/11/22
1268	**Router test and soak**	**1 day**	**Mon 2/28/22**	**Mon 2/28/22**
1269	Router monitoring and management initiated	1 day	Mon 2/28/22	Mon 2/28/22
1270	Documentation of monitoring and management system	1 day	Mon 2/28/22	Mon 2/28/22
1271	Router cut over	1 day	Mon 3/14/22	Mon 3/14/22
1272	Redline Design Changes Documented	10 days	Tue 3/1/22	Mon 3/14/22
1273	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Fri 8/6/21**	**Thu 9/2/21**
1274	Cable estimates	1 day	Fri 8/6/21	Fri 8/6/21
1275	Cable design complete	5 days	Fri 8/6/21	Thu 8/12/21

ID	Task Name	Duration	Start	Finish
1276	Run cable	10 days	Mon 8/9/21	Fri 8/20/21
1277	Cable Termination	10 days	Fri 8/13/21	Thu 8/26/21
1278	Test LAN WAN	5 days	Mon 8/23/21	Fri 8/27/21
1279	Install VoIP Phone	5 days	Fri 8/27/21	Thu 9/2/21
1280	Ready for service	0 days	Thu 9/2/21	Thu 9/2/21
1281	**Network Readiness Complete**	**126 days**	**Thu 9/2/21**	**Fri 2/25/22**
1282	NID installed	0 days	Thu 9/2/21	Thu 9/2/21
1283	VLAN Provisioning Complete	0 days	Thu 9/2/21	Thu 9/2/21
1284	CPE Equipment Installed	0 days	Thu 9/2/21	Thu 9/2/21
1285	**Tertiary network established (Commodity Internet)**	**61 days**	**Fri 12/3/21**	**Fri 2/25/22**
1286	Tertiary network services documented	5 days	Fri 12/3/21	Thu 12/9/21
1287	Tertiary network services designed	10 days	Fri 12/10/21	Thu 12/23/21
1288	Tertiary network services ordered	1 day	Fri 12/24/21	Fri 12/24/21
1289	Tertiary network services installed	30 days	Mon 12/27/21	Fri 2/4/22
1290	Tertiary network services tested	15 days	Mon 2/7/22	Fri 2/25/22
1291	**Admin/PCAP Server (as required)**	**131 days**	**Thu 8/5/21**	**Thu 2/3/22**
1292	Admin/PCAP connections documented	45 days	Fri 12/3/21	Thu 2/3/22
1293	Admin/PCAP connections designed and installed, initial test	30 days	Fri 9/3/21	Thu 10/14/21
1294	Admin/PCAP SIP turned up and tested, final test	1 day	Thu 8/5/21	Thu 8/5/21

ID	Task Name	Duration	Start	Finish
1295	**LNG Design (audio codes - as required)**	**51 days**	**Fri 8/6/21**	**Fri 10/15/21**
1296	LNG design completed	10 days	Fri 8/6/21	Thu 8/19/21
1297	LNG ordered	1 day	Fri 8/20/21	Fri 8/20/21
1298	LNG recieved	30 days	Mon 8/23/21	Fri 10/1/21
1299	LNG configured, installed, and initial testing	10 days	Mon 10/4/21	Fri 10/15/21
1300	**911 MEVO (optional) connections**	**102 days**	**Fri 12/3/21**	**Mon 4/25/22**
1301	MEVO connections documented	15 days	Fri 12/3/21	Thu 12/23/21
1302	MEVO connections designed and installed	30 days	Tue 3/15/22	Mon 4/25/22
1303	MEVO Phone turned up and tested	5 days	Fri 12/24/21	Thu 12/30/21
1304	**RCH Readiness Certification**	**205 days**	**Tue 8/10/21**	**Mon 5/23/22**
1305	Final Design Documented	5 days	Fri 9/3/21	Thu 9/9/21
1306	**Test Plan Completion**	**125 days**	**Mon 8/23/21**	**Fri 2/11/22**
1307	**RCH routers**	**125 days**	**Mon 8/23/21**	**Fri 2/11/22**
1308	**WAN validation and failover**	**125 days**	**Mon 8/23/21**	**Fri 2/11/22**
1309	Primary	5 days	Mon 8/23/21	Fri 8/27/21
1310	Secondary	5 days	Mon 8/23/21	Fri 8/27/21
1311	Tertiary	5 days	Mon 2/7/22	Fri 2/11/22
1312	**ESRP Software Applications**	**205 days**	**Tue 8/10/21**	**Mon 5/23/22**
1313	**ESRP Operational**	**30 days**	**Tue 8/10/21**	**Mon 9/20/21**
1314	Policy Routing	30 days	Tue 8/10/21	Mon 9/20/21
1315	**Policy Routing Failover**	**5 days**	**Tue 9/21/21**	**Mon 9/27/21**
1316	Primary failover	5 days	Tue 9/21/21	Mon 9/27/21
1317	Secondary failover	5 days	Tue 9/21/21	Mon 9/27/21
1318	Admin failover	5 days	Tue 9/21/21	Mon 9/27/21
1319	MEVO (optional) failover	5 days	Tue 9/21/21	Mon 9/27/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
1320	**Database operational**	**1 day**	**Tue 9/21/21**	**Tue 9/21/21**
1321	SRDB transitional conversion documented	1 day	Tue 9/21/21	Tue 9/21/21
1322	**RCH toolkit Application**	**21 days**	**Tue 9/21/21**	**Tue 10/19/21**
1323	Tool kit credentials documented	10 days	Tue 9/21/21	Mon 10/4/21
1324	Tool kit RCH setup complete	10 days	Tue 10/5/21	Mon 10/18/21
1325	Tool kit verified	1 day	Tue 10/19/21	Tue 10/19/21
1326	Training	20 days	Tue 4/26/22	Mon 5/23/22
1327	**Carrier Network Conversion**	**111 days**	**Mon 10/4/21**	**Mon 3/7/22**
1328	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Mon 10/4/21	Fri 10/8/21
1329	Phase 1B - Confirm CPE Cutover Date	5 days	Mon 12/13/21	Fri 12/17/21
1330	Phase 2 - ESRP Configuration	45 days	Mon 10/11/21	Fri 12/10/21
1331	Phase 3A - Carrier Trunks installed	0 days	Fri 12/10/21	Fri 12/10/21
1332	**Phase 3B - Carrier conversion**	**61 days**	**Mon 12/13/21**	**Mon 3/7/22**
1333	Wireless Conversion	1 day	Mon 12/13/21	Mon 12/13/21
1334	Wireline Conversion	60 days	Tue 12/14/21	Mon 3/7/22
1335	RCH Closeout Complete	0 days	Mon 5/23/22	Mon 5/23/22
1336	**North East Region (in development)**	**382 days**	**Fri 12/25/20**	**Mon 6/13/22**
1337	**WAN Testing**	**15 days**	**Mon 7/5/21**	**Fri 7/23/21**
1349	**Network Conversion Capability Turn-up**	**186 days**	**Fri 12/25/20**	**Fri 9/10/21**
1371	**OSP Service Conversion**	**138 days**	**Fri 2/5/21**	**Tue 8/17/21**
1386	**Norfolk RCH**	**208 days**	**Wed 8/18/21**	**Fri 6/3/22**
1387	**RCH Physical Network Configuration**	**188 days**	**Wed 8/18/21**	**Fri 5/6/22**
1388	Project Kick Off	1 day	Wed 8/18/21	Wed 8/18/21
1389	**Site Survey**	**2 days**	**Thu 8/19/21**	**Fri 8/20/21**

ID	Task Name	Duration	Start	Finish
1390	RCH Survey and Questionnaire Received	1 day	Thu 8/19/21	Thu 8/19/21
1391	Survey Documentation Received	1 day	Fri 8/20/21	Fri 8/20/21
1392	Initial RCH design	15 days	Thu 8/19/21	Wed 9/8/21
1393	Texty (optional) confirmed	15 days	Thu 8/19/21	Wed 9/8/21
1394	Rack assignments	15 days	Thu 8/19/21	Wed 9/8/21
1395	LAN assignments	15 days	Thu 8/19/21	Wed 9/8/21
1396	WAN assignments	15 days	Thu 8/19/21	Wed 9/8/21
1397	**Call Flow Design**	**85 days**	**Thu 8/19/21**	**Wed 12/15/21**
1398	Call routing documentation complete	85 days	Thu 8/19/21	Wed 12/15/21
1399	Call flow logical diagram complete	85 days	Thu 8/19/21	Wed 12/15/21
1400	Initial Design Sign Off	10 days	Fri 8/20/21	Thu 9/2/21
1401	**RCH router documentation**	**72 days**	**Thu 12/16/21**	**Fri 3/25/22**
1402	Configuration specs	15 days	Thu 12/16/21	Wed 1/5/22
1403	Router equipment order	1 day	Thu 1/6/22	Thu 1/6/22
1404	Router received	30 days	Fri 1/7/22	Thu 2/17/22
1405	Router build and stage	15 days	Fri 2/18/22	Thu 3/10/22
1406	Router installation	10 days	Fri 3/11/22	Thu 3/24/22
1407	**Router test and soak**	**1 day**	**Fri 3/11/22**	**Fri 3/11/22**
1408	Router monitoring and management initiated	1 day	Fri 3/11/22	Fri 3/11/22
1409	Documentation of monitoring and management system	1 day	Fri 3/11/22	Fri 3/11/22
1410	Router cut over	1 day	Fri 3/25/22	Fri 3/25/22
1411	Redline Design Changes Documented	10 days	Mon 3/14/22	Fri 3/25/22

ID	Task Name	Duration	Start	Finish
1412	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Thu 8/19/21**	**Wed 9/15/21**
1413	Cable estimates	1 day	Thu 8/19/21	Thu 8/19/21
1414	Cable design complete	5 days	Thu 8/19/21	Wed 8/25/21
1415	Run cable	10 days	Fri 8/20/21	Thu 9/2/21
1416	Cable Termination	10 days	Thu 8/26/21	Wed 9/8/21
1417	Test LAN WAN	5 days	Fri 9/3/21	Thu 9/9/21
1418	Install VoIP Phone	5 days	Thu 9/9/21	Wed 9/15/21
1419	Ready for service	0 days	Wed 9/15/21	Wed 9/15/21
1420	**Network Readiness Complete**	**126 days**	**Wed 9/15/21**	**Thu 3/10/22**
1421	NID installed	0 days	Wed 9/15/21	Wed 9/15/21
1422	VLAN Provisioning Complete	0 days	Wed 9/15/21	Wed 9/15/21
1423	CPE Equipment Installed	0 days	Wed 9/15/21	Wed 9/15/21
1424	**Tertiary network established (Commodity Internet)**	**61 days**	**Thu 12/16/21**	**Thu 3/10/22**
1425	Tertiary network services documented	5 days	Thu 12/16/21	Wed 12/22/21
1426	Tertiary network services designed	10 days	Thu 12/23/21	Wed 1/5/22
1427	Tertiary network services ordered	1 day	Thu 1/6/22	Thu 1/6/22
1428	Tertiary network services installed	30 days	Fri 1/7/22	Thu 2/17/22
1429	Tertiary network services tested	15 days	Fri 2/18/22	Thu 3/10/22
1430	**Admin/PCAP Server (as required)**	**131 days**	**Wed 8/18/21**	**Wed 2/16/22**
1431	Admin/PCAP connections documented	45 days	Thu 12/16/21	Wed 2/16/22

ID	Task Name	Duration	Start	Finish
1432	Admin/PCAP connections designed and installed, initial test	30 days	Thu 9/16/21	Wed 10/27/21
1433	Admin/PCAP SIP turned up and tested, final test	1 day	Wed 8/18/21	Wed 8/18/21
1434	**LNG Design (audio codes - as required)**	**51 days**	**Thu 8/19/21**	**Thu 10/28/21**
1435	LNG design completed	10 days	Thu 8/19/21	Wed 9/1/21
1436	LNG ordered	1 day	Thu 9/2/21	Thu 9/2/21
1437	LNG recieved	30 days	Fri 9/3/21	Thu 10/14/21
1438	LNG configured, installed, and initial testing	10 days	Fri 10/15/21	Thu 10/28/21
1439	**911 MEVO (optional) connections**	**102 days**	**Thu 12/16/21**	**Fri 5/6/22**
1440	MEVO connections documented	15 days	Thu 12/16/21	Wed 1/5/22
1441	MEVO connections designed and installed	30 days	Mon 3/28/22	Fri 5/6/22
1442	MEVO Phone turned up and tested	5 days	Thu 1/6/22	Wed 1/12/22
1443	**RCH Readiness Certification**	**205 days**	**Mon 8/23/21**	**Fri 6/3/22**
1444	Final Design Documented	5 days	Thu 9/16/21	Wed 9/22/21
1445	**Test Plan Completion**	**125 days**	**Fri 9/3/21**	**Thu 2/24/22**
1446	**RCH routers**	**125 days**	**Fri 9/3/21**	**Thu 2/24/22**
1447	**WAN validation and failover**	**125 days**	**Fri 9/3/21**	**Thu 2/24/22**
1448	Primary	5 days	Fri 9/3/21	Thu 9/9/21
1449	Secondary	5 days	Fri 9/3/21	Thu 9/9/21
1450	Tertiary	5 days	Fri 2/18/22	Thu 2/24/22
1451	**ESRP Software Applications**	**205 days**	**Mon 8/23/21**	**Fri 6/3/22**
1452	**ESRP Operational**	**30 days**	**Mon 8/23/21**	**Fri 10/1/21**
1453	Policy Routing	30 days	Mon 8/23/21	Fri 10/1/21

Ne RFP Project Plan

ID	Task Name	Duration	Start	Finish
1454	**Policy Routing Failover**	**5 days**	**Mon 10/4/21**	**Fri 10/8/21**
1455	Primary failover	5 days	Mon 10/4/21	Fri 10/8/21
1456	Secondary failover	5 days	Mon 10/4/21	Fri 10/8/21
1457	Admin failover	5 days	Mon 10/4/21	Fri 10/8/21
1458	MEVO (optional) failover	5 days	Mon 10/4/21	Fri 10/8/21
1459	**Database operational**	**1 day**	**Mon 10/4/21**	**Mon 10/4/21**
1460	SRDB transitional conversion documented	1 day	Mon 10/4/21	Mon 10/4/21
1461	**RCH toolkit Application**	**21 days**	**Mon 10/4/21**	**Mon 11/1/21**
1462	Tool kit credentials documented	10 days	Mon 10/4/21	Fri 10/15/21
1463	Tool kit RCH setup complete	10 days	Mon 10/18/21	Fri 10/29/21
1464	Tool kit verified	1 day	Mon 11/1/21	Mon 11/1/21
1465	Training	20 days	Mon 5/9/22	Fri 6/3/22
1466	**Carrier Network Conversion**	**111 days**	**Fri 10/15/21**	**Fri 3/18/22**
1467	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Fri 10/15/21	Thu 10/21/21
1468	Phase 1B - Confirm CPE Cutover Date	5 days	Fri 12/24/21	Thu 12/30/21
1469	Phase 2 - ESRP Configuration	45 days	Fri 10/22/21	Thu 12/23/21
1470	Phase 3A - Carrier Trunks installed	0 days	Thu 12/23/21	Thu 12/23/21
1471	**Phase 3B - Carrier conversion**	**61 days**	**Fri 12/24/21**	**Fri 3/18/22**
1472	Wireless Conversion	1 day	Fri 12/24/21	Fri 12/24/21
1473	Wireline Conversion	60 days	Mon 12/27/21	Fri 3/18/22
1474	RCH Closeout Complete	0 days	Fri 6/3/22	Fri 6/3/22
1475	**South Sioux City RCH**	**208 days**	**Thu 8/26/21**	**Mon 6/13/22**
1476	**RCH Physical Network Configuration**	**188 days**	**Thu 8/26/21**	**Mon 5/16/22**
1477	Project Kick Off	1 day	Thu 8/26/21	Thu 8/26/21

ID	Task Name	Duration	Start	Finish
1478	**Site Survey**	**2 days**	**Fri 8/27/21**	**Mon 8/30/21**
1479	RCH Survey and Questionnaire Received	1 day	Fri 8/27/21	Fri 8/27/21
1480	Survey Documentation Received	1 day	Mon 8/30/21	Mon 8/30/21
1481	Initial RCH design	15 days	Fri 8/27/21	Thu 9/16/21
1482	Texty (optional) confirmed	15 days	Fri 8/27/21	Thu 9/16/21
1483	Rack assignments	15 days	Fri 8/27/21	Thu 9/16/21
1484	LAN assignments	15 days	Fri 8/27/21	Thu 9/16/21
1485	WAN assignments	15 days	Fri 8/27/21	Thu 9/16/21
1486	**Call Flow Design**	**85 days**	**Fri 8/27/21**	**Thu 12/23/21**
1487	Call routing documentation complete	85 days	Fri 8/27/21	Thu 12/23/21
1488	Call flow logical diagram complete	85 days	Fri 8/27/21	Thu 12/23/21
1489	Initial Design Sign Off	10 days	Mon 8/30/21	Fri 9/10/21
1490	**RCH router documentation**	**72 days**	**Fri 12/24/21**	**Mon 4/4/22**
1491	Configuration specs	15 days	Fri 12/24/21	Thu 1/13/22
1492	Router equipment order	1 day	Fri 1/14/22	Fri 1/14/22
1493	Router received	30 days	Mon 1/17/22	Fri 2/25/22
1494	Router build and stage	15 days	Mon 2/28/22	Fri 3/18/22
1495	Router installation	10 days	Mon 3/21/22	Fri 4/1/22
1496	**Router test and soak**	**1 day**	**Mon 3/21/22**	**Mon 3/21/22**
1497	Router monitoring and management initiated	1 day	Mon 3/21/22	Mon 3/21/22
1498	Documentation of monitoring and management system	1 day	Mon 3/21/22	Mon 3/21/22
1499	Router cut over	1 day	Mon 4/4/22	Mon 4/4/22

ID	Task Name	Duration	Start	Finish
1500	Redline Design Changes Documented	10 days	Tue 3/22/22	Mon 4/4/22
1501	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Fri 8/27/21**	**Thu 9/23/21**
1502	Cable estimates	1 day	Fri 8/27/21	Fri 8/27/21
1503	Cable design complete	5 days	Fri 8/27/21	Thu 9/2/21
1504	Run cable	10 days	Mon 8/30/21	Fri 9/10/21
1505	Cable Termination	10 days	Fri 9/3/21	Thu 9/16/21
1506	Test LAN WAN	5 days	Mon 9/13/21	Fri 9/17/21
1507	Install VoIP Phone	5 days	Fri 9/17/21	Thu 9/23/21
1508	Ready for service	0 days	Thu 9/23/21	Thu 9/23/21
1509	**Network Readiness Complete**	**126 days**	**Thu 9/23/21**	**Fri 3/18/22**
1510	NID installed	0 days	Thu 9/23/21	Thu 9/23/21
1511	VLAN Provisioning Complete	0 days	Thu 9/23/21	Thu 9/23/21
1512	CPE Equipment Installed	0 days	Thu 9/23/21	Thu 9/23/21
1513	**Tertiary network established (Commodity Internet)**	**61 days**	**Fri 12/24/21**	**Fri 3/18/22**
1514	Tertiary network services documented	5 days	Fri 12/24/21	Thu 12/30/21
1515	Tertiary network services designed	10 days	Fri 12/31/21	Thu 1/13/22
1516	Tertiary network services ordered	1 day	Fri 1/14/22	Fri 1/14/22
1517	Tertiary network services installed	30 days	Mon 1/17/22	Fri 2/25/22
1518	Tertiary network services tested	15 days	Mon 2/28/22	Fri 3/18/22
1519	**Admin/PCAP Server (as required)**	**131 days**	**Thu 8/26/21**	**Thu 2/24/22**
1520	Admin/PCAP connections documented	45 days	Fri 12/24/21	Thu 2/24/22

ID	Task Name	Duration	Start	Finish
1521	Admin/PCAP connections designed and installed, initial test	30 days	Fri 9/24/21	Thu 11/4/21
1522	Admin/PCAP SIP turned up and tested, final test	1 day	Thu 8/26/21	Thu 8/26/21
1523	**LNG Design (audio codes - as required)**	**51 days**	**Fri 8/27/21**	**Fri 11/5/21**
1524	LNG design completed	10 days	Fri 8/27/21	Thu 9/9/21
1525	LNG ordered	1 day	Fri 9/10/21	Fri 9/10/21
1526	LNG recieved	30 days	Mon 9/13/21	Fri 10/22/21
1527	LNG configured, installed, and initial testing	10 days	Mon 10/25/21	Fri 11/5/21
1528	**911 MEVO (optional) connections**	**102 days**	**Fri 12/24/21**	**Mon 5/16/22**
1529	MEVO connections documented	15 days	Fri 12/24/21	Thu 1/13/22
1530	MEVO connections designed and installed	30 days	Tue 4/5/22	Mon 5/16/22
1531	MEVO Phone turned up and tested	5 days	Fri 1/14/22	Thu 1/20/22
1532	**RCH Readiness Certification**	**205 days**	**Tue 8/31/21**	**Mon 6/13/22**
1533	Final Design Documented	5 days	Fri 9/24/21	Thu 9/30/21
1534	**Test Plan Completion**	**125 days**	**Mon 9/13/21**	**Fri 3/4/22**
1535	**RCH routers**	**125 days**	**Mon 9/13/21**	**Fri 3/4/22**
1536	**WAN validation and failover**	**125 days**	**Mon 9/13/21**	**Fri 3/4/22**
1537	Primary	5 days	Mon 9/13/21	Fri 9/17/21
1538	Secondary	5 days	Mon 9/13/21	Fri 9/17/21
1539	Tertiary	5 days	Mon 2/28/22	Fri 3/4/22
1540	**ESRP Software Applications**	**205 days**	**Tue 8/31/21**	**Mon 6/13/22**
1541	**ESRP Operational**	**30 days**	**Tue 8/31/21**	**Mon 10/11/21**
1542	Policy Routing	30 days	Tue 8/31/21	Mon 10/11/21

ID	Task Name	Duration	Start	Finish
1543	**Policy Routing Failover**	**5 days**	**Tue 10/12/21**	**Mon 10/18/21**
1544	Primary failover	5 days	Tue 10/12/21	Mon 10/18/21
1545	Secondary failover	5 days	Tue 10/12/21	Mon 10/18/21
1546	Admin failover	5 days	Tue 10/12/21	Mon 10/18/21
1547	MEVO (optional) failover	5 days	Tue 10/12/21	Mon 10/18/21
1548	**Database operational**	**1 day**	**Tue 10/12/21**	**Tue 10/12/21**
1549	SRDB transitional conversion documented	1 day	Tue 10/12/21	Tue 10/12/21
1550	**RCH toolkit Application**	**21 days**	**Tue 10/12/21**	**Tue 11/9/21**
1551	Tool kit credentials documented	10 days	Tue 10/12/21	Mon 10/25/21
1552	Tool kit RCH setup complete	10 days	Tue 10/26/21	Mon 11/8/21
1553	Tool kit verified	1 day	Tue 11/9/21	Tue 11/9/21
1554	Training	20 days	Tue 5/17/22	Mon 6/13/22
1555	**Carrier Network Conversion**	**111 days**	**Mon 10/25/21**	**Mon 3/28/22**
1556	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Mon 10/25/21	Fri 10/29/21
1557	Phase 1B - Confirm CPE Cutover Date	5 days	Mon 1/3/22	Fri 1/7/22
1558	Phase 2 - ESRP Configuration	45 days	Mon 11/1/21	Fri 12/31/21
1559	Phase 3A - Carrier Trunks installed	0 days	Fri 12/31/21	Fri 12/31/21
1560	**Phase 3B - Carrier conversion**	**61 days**	**Mon 1/3/22**	**Mon 3/28/22**
1561	Wireless Conversion	1 day	Mon 1/3/22	Mon 1/3/22
1562	Wireline Conversion	60 days	Tue 1/4/22	Mon 3/28/22
1563	RCH Closeout Complete	0 days	Mon 6/13/22	Mon 6/13/22
1564	**Metro West Region (in development)**	**397 days**	**Fri 12/25/20**	**Mon 7/4/22**
1565	**WAN Testing**	**15 days**	**Mon 7/26/21**	**Fri 8/13/21**
1577	**Network Conversion Capability Turn-up**	**201 days**	**Fri 12/25/20**	**Fri 10/1/21**

ID	Task Name	Duration	Start	Finish
1599	**OSP Service Conversion**	**153 days**	**Fri 2/5/21**	**Tue 9/7/21**
1614	**Fremont/Dodge County 911 RCH**	**208 days**	**Wed 9/8/21**	**Fri 6/24/22**
1615	**RCH Physical Network Configuration**	**188 days**	**Wed 9/8/21**	**Fri 5/27/22**
1616	Project Kick Off	1 day	Wed 9/8/21	Wed 9/8/21
1617	**Site Survey**	**2 days**	**Thu 9/9/21**	**Fri 9/10/21**
1618	RCH Survey and Questionnaire Received	1 day	Thu 9/9/21	Thu 9/9/21
1619	Survey Documentation Received	1 day	Fri 9/10/21	Fri 9/10/21
1620	Initial RCH design	15 days	Thu 9/9/21	Wed 9/29/21
1621	Texty (optional) confirmed	15 days	Thu 9/9/21	Wed 9/29/21
1622	Rack assignments	15 days	Thu 9/9/21	Wed 9/29/21
1623	LAN assignments	15 days	Thu 9/9/21	Wed 9/29/21
1624	WAN assignments	15 days	Thu 9/9/21	Wed 9/29/21
1625	**Call Flow Design**	**85 days**	**Thu 9/9/21**	**Wed 1/5/22**
1626	Call routing documentation complete	85 days	Thu 9/9/21	Wed 1/5/22
1627	Call flow logical diagram complete	85 days	Thu 9/9/21	Wed 1/5/22
1628	Initial Design Sign Off	10 days	Fri 9/10/21	Thu 9/23/21
1629	**RCH router documentation**	**72 days**	**Thu 1/6/22**	**Fri 4/15/22**
1630	Configuration specs	15 days	Thu 1/6/22	Wed 1/26/22
1631	Router equipment order	1 day	Thu 1/27/22	Thu 1/27/22
1632	Router received	30 days	Fri 1/28/22	Thu 3/10/22
1633	Router build and stage	15 days	Fri 3/11/22	Thu 3/31/22
1634	Router installation	10 days	Fri 4/1/22	Thu 4/14/22
1635	**Router test and soak**	**1 day**	**Fri 4/1/22**	**Fri 4/1/22**
1636	Router monitoring and management initiated	1 day	Fri 4/1/22	Fri 4/1/22

ID	Task Name	Duration	Start	Finish
1637	Documentation of monitoring and management system	1 day	Fri 4/1/22	Fri 4/1/22
1638	Router cut over	1 day	Fri 4/15/22	Fri 4/15/22
1639	Redline Design Changes Documented	10 days	Mon 4/4/22	Fri 4/15/22
1640	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Thu 9/9/21**	**Wed 10/6/21**
1641	Cable estimates	1 day	Thu 9/9/21	Thu 9/9/21
1642	Cable design complete	5 days	Thu 9/9/21	Wed 9/15/21
1643	Run cable	10 days	Fri 9/10/21	Thu 9/23/21
1644	Cable Termination	10 days	Thu 9/16/21	Wed 9/29/21
1645	Test LAN WAN	5 days	Fri 9/24/21	Thu 9/30/21
1646	Install VoIP Phone	5 days	Thu 9/30/21	Wed 10/6/21
1647	Ready for service	0 days	Wed 10/6/21	Wed 10/6/21
1648	**Network Readiness Complete**	**126 days**	**Wed 10/6/21**	**Thu 3/31/22**
1649	NID installed	0 days	Wed 10/6/21	Wed 10/6/21
1650	VLAN Provisioning Complete	0 days	Wed 10/6/21	Wed 10/6/21
1651	CPE Equipment Installed	0 days	Wed 10/6/21	Wed 10/6/21
1652	**Tertiary network established (Commodity Internet)**	**61 days**	**Thu 1/6/22**	**Thu 3/31/22**
1653	Tertiary network services documented	5 days	Thu 1/6/22	Wed 1/12/22
1654	Tertiary network services designed	10 days	Thu 1/13/22	Wed 1/26/22
1655	Tertiary network services ordered	1 day	Thu 1/27/22	Thu 1/27/22
1656	Tertiary network services installed	30 days	Fri 1/28/22	Thu 3/10/22

ID	Task Name	Duration	Start	Finish
1657	Tertiary network services tested	15 days	Fri 3/11/22	Thu 3/31/22
1658	**Admin/PCAP Server (as required)**	**131 days**	**Wed 9/8/21**	**Wed 3/9/22**
1659	Admin/PCAP connections documented	45 days	Thu 1/6/22	Wed 3/9/22
1660	Admin/PCAP connections designed and installed, initial test	30 days	Thu 10/7/21	Wed 11/17/21
1661	Admin/PCAP SIP turned up and tested, final test	1 day	Wed 9/8/21	Wed 9/8/21
1662	**LNG Design (audio codes - as required)**	**51 days**	**Thu 9/9/21**	**Thu 11/18/21**
1663	LNG design completed	10 days	Thu 9/9/21	Wed 9/22/21
1664	LNG ordered	1 day	Thu 9/23/21	Thu 9/23/21
1665	LNG recieved	30 days	Fri 9/24/21	Thu 11/4/21
1666	LNG configured, installed, and initial testing	10 days	Fri 11/5/21	Thu 11/18/21
1667	**911 MEVO (optional) connections**	**102 days**	**Thu 1/6/22**	**Fri 5/27/22**
1668	MEVO connections documented	15 days	Thu 1/6/22	Wed 1/26/22
1669	MEVO connections designed and installed	30 days	Mon 4/18/22	Fri 5/27/22
1670	MEVO Phone turned up and tested	5 days	Thu 1/27/22	Wed 2/2/22
1671	**RCH Readiness Certification**	**205 days**	**Mon 9/13/21**	**Fri 6/24/22**
1672	Final Design Documented	5 days	Thu 10/7/21	Wed 10/13/21
1673	**Test Plan Completion**	**125 days**	**Fri 9/24/21**	**Thu 3/17/22**
1674	**RCH routers**	**125 days**	**Fri 9/24/21**	**Thu 3/17/22**
1675	**WAN validation and failover**	**125 days**	**Fri 9/24/21**	**Thu 3/17/22**
1676	Primary	5 days	Fri 9/24/21	Thu 9/30/21

ID	Task Name	Duration	Start	Finish
1677	Secondary	5 days	Fri 9/24/21	Thu 9/30/21
1678	Tertiary	5 days	Fri 3/11/22	Thu 3/17/22
1679	**ESRP Software Applications**	**205 days**	**Mon 9/13/21**	**Fri 6/24/22**
1680	**ESRP Operational**	**30 days**	**Mon 9/13/21**	**Fri 10/22/21**
1681	Policy Routing	30 days	Mon 9/13/21	Fri 10/22/21
1682	**Policy Routing Failover**	**5 days**	**Mon 10/25/21**	**Fri 10/29/21**
1683	Primary failover	5 days	Mon 10/25/21	Fri 10/29/21
1684	Secondary failover	5 days	Mon 10/25/21	Fri 10/29/21
1685	Admin failover	5 days	Mon 10/25/21	Fri 10/29/21
1686	MEVO (optional) failover	5 days	Mon 10/25/21	Fri 10/29/21
1687	**Database operational**	**1 day**	**Mon 10/25/21**	**Mon 10/25/21**
1688	SRDB transitional conversion documented	1 day	Mon 10/25/21	Mon 10/25/21
1689	**RCH toolkit Application**	**21 days**	**Mon 10/25/21**	**Mon 11/22/21**
1690	Tool kit credentials documented	10 days	Mon 10/25/21	Fri 11/5/21
1691	Tool kit RCH setup complete	10 days	Mon 11/8/21	Fri 11/19/21
1692	Tool kit verified	1 day	Mon 11/22/21	Mon 11/22/21
1693	Training	20 days	Mon 5/30/22	Fri 6/24/22
1694	**Carrier Network Conversion**	**111 days**	**Fri 11/5/21**	**Fri 4/8/22**
1695	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Fri 11/5/21	Thu 11/11/21
1696	Phase 1B - Confirm CPE Cutover Date	5 days	Fri 1/14/22	Thu 1/20/22
1697	Phase 2 - ESRP Configuration	45 days	Fri 11/12/21	Thu 1/13/22
1698	Phase 3A - Carrier Trunks installed	0 days	Thu 1/13/22	Thu 1/13/22
1699	**Phase 3B - Carrier conversion**	**61 days**	**Fri 1/14/22**	**Fri 4/8/22**
1700	Wireless Conversion	1 day	Fri 1/14/22	Fri 1/14/22

ID	Task Name	Duration	Start	Finish
1701	Wireline Conversion	60 days	Mon 1/17/22	Fri 4/8/22
1702	RCH Closeout Complete	0 days	Fri 6/24/22	Fri 6/24/22
1703	**Colfax County 911 RCH**	**208 days**	**Thu 9/16/21**	**Mon 7/4/22**
1704	**RCH Physical Network Configuration**	**188 days**	**Thu 9/16/21**	**Mon 6/6/22**
1705	Project Kick Off	1 day	Thu 9/16/21	Thu 9/16/21
1706	**Site Survey**	**2 days**	**Fri 9/17/21**	**Mon 9/20/21**
1707	RCH Survey and Questionnaire Received	1 day	Fri 9/17/21	Fri 9/17/21
1708	Survey Documentation Received	1 day	Mon 9/20/21	Mon 9/20/21
1709	Initial RCH design	15 days	Fri 9/17/21	Thu 10/7/21
1710	Texty (optional) confirmed	15 days	Fri 9/17/21	Thu 10/7/21
1711	Rack assignments	15 days	Fri 9/17/21	Thu 10/7/21
1712	LAN assignments	15 days	Fri 9/17/21	Thu 10/7/21
1713	WAN assignments	15 days	Fri 9/17/21	Thu 10/7/21
1714	**Call Flow Design**	**85 days**	**Fri 9/17/21**	**Thu 1/13/22**
1715	Call routing documentation complete	85 days	Fri 9/17/21	Thu 1/13/22
1716	Call flow logical diagram complete	85 days	Fri 9/17/21	Thu 1/13/22
1717	Initial Design Sign Off	10 days	Mon 9/20/21	Fri 10/1/21
1718	**RCH router documentation**	**72 days**	**Fri 1/14/22**	**Mon 4/25/22**
1719	Configuration specs	15 days	Fri 1/14/22	Thu 2/3/22
1720	Router equipment order	1 day	Fri 2/4/22	Fri 2/4/22
1721	Router received	30 days	Mon 2/7/22	Fri 3/18/22
1722	Router build and stage	15 days	Mon 3/21/22	Fri 4/8/22
1723	Router installation	10 days	Mon 4/11/22	Fri 4/22/22
1724	**Router test and soak**	**1 day**	**Mon 4/11/22**	**Mon 4/11/22**
1725	Router monitoring and management initiated	1 day	Mon 4/11/22	Mon 4/11/22

ID	Task Name	Duration	Start	Finish
1726	Documentation of monitoring and management system	1 day	Mon 4/11/22	Mon 4/11/22
1727	Router cut over	1 day	Mon 4/25/22	Mon 4/25/22
1728	Redline Design Changes Documented	10 days	Tue 4/12/22	Mon 4/25/22
1729	**RCH MEVO (optional) Cabling (as required)**	**20 days**	**Fri 9/17/21**	**Thu 10/14/21**
1730	Cable estimates	1 day	Fri 9/17/21	Fri 9/17/21
1731	Cable design complete	5 days	Fri 9/17/21	Thu 9/23/21
1732	Run cable	10 days	Mon 9/20/21	Fri 10/1/21
1733	Cable Termination	10 days	Fri 9/24/21	Thu 10/7/21
1734	Test LAN WAN	5 days	Mon 10/4/21	Fri 10/8/21
1735	Install VoIP Phone	5 days	Fri 10/8/21	Thu 10/14/21
1736	Ready for service	0 days	Thu 10/14/21	Thu 10/14/21
1737	**Network Readiness Complete**	**126 days**	**Thu 10/14/21**	**Fri 4/8/22**
1738	NID installed	0 days	Thu 10/14/21	Thu 10/14/21
1739	VLAN Provisioning Complete	0 days	Thu 10/14/21	Thu 10/14/21
1740	CPE Equipment Installed	0 days	Thu 10/14/21	Thu 10/14/21
1741	**Tertiary network established (Commodity Internet)**	**61 days**	**Fri 1/14/22**	**Fri 4/8/22**
1742	Tertiary network services documented	5 days	Fri 1/14/22	Thu 1/20/22
1743	Tertiary network services designed	10 days	Fri 1/21/22	Thu 2/3/22
1744	Tertiary network services ordered	1 day	Fri 2/4/22	Fri 2/4/22
1745	Tertiary network services installed	30 days	Mon 2/7/22	Fri 3/18/22

ID	Task Name	Duration	Start	Finish
1746	Tertiary network services tested	15 days	Mon 3/21/22	Fri 4/8/22
1747	**Admin/PCAP Server (as required)**	**131 days**	**Thu 9/16/21**	**Thu 3/17/22**
1748	Admin/PCAP connections documented	45 days	Fri 1/14/22	Thu 3/17/22
1749	Admin/PCAP connections designed and installed, initial test	30 days	Fri 10/15/21	Thu 11/25/21
1750	Admin/PCAP SIP turned up and tested, final test	1 day	Thu 9/16/21	Thu 9/16/21
1751	**LNG Design (audio codes - as required)**	**51 days**	**Fri 9/17/21**	**Fri 11/26/21**
1752	LNG design completed	10 days	Fri 9/17/21	Thu 9/30/21
1753	LNG ordered	1 day	Fri 10/1/21	Fri 10/1/21
1754	LNG recieved	30 days	Mon 10/4/21	Fri 11/12/21
1755	LNG configured, installed, and initial testing	10 days	Mon 11/15/21	Fri 11/26/21
1756	**911 MEVO (optional) connections**	**102 days**	**Fri 1/14/22**	**Mon 6/6/22**
1757	MEVO connections documented	15 days	Fri 1/14/22	Thu 2/3/22
1758	MEVO connections designed and installed	30 days	Tue 4/26/22	Mon 6/6/22
1759	MEVO Phone turned up and tested	5 days	Fri 2/4/22	Thu 2/10/22
1760	**RCH Readiness Certification**	**205 days**	**Tue 9/21/21**	**Mon 7/4/22**
1761	Final Design Documented	5 days	Fri 10/15/21	Thu 10/21/21
1762	**Test Plan Completion**	**125 days**	**Mon 10/4/21**	**Fri 3/25/22**
1763	**RCH routers**	**125 days**	**Mon 10/4/21**	**Fri 3/25/22**
1764	**WAN validation and failover**	**125 days**	**Mon 10/4/21**	**Fri 3/25/22**
1765	Primary	5 days	Mon 10/4/21	Fri 10/8/21

ID	Task Name	Duration	Start	Finish
1766	Secondary	5 days	Mon 10/4/21	Fri 10/8/21
1767	Tertiary	5 days	Mon 3/21/22	Fri 3/25/22
1768	**ESRP Software Applications**	**205 days**	**Tue 9/21/21**	**Mon 7/4/22**
1769	**ESRP Operational**	**30 days**	**Tue 9/21/21**	**Mon 11/1/21**
1770	Policy Routing	30 days	Tue 9/21/21	Mon 11/1/21
1771	**Policy Routing Failover**	**5 days**	**Tue 11/2/21**	**Mon 11/8/21**
1772	Primary failover	5 days	Tue 11/2/21	Mon 11/8/21
1773	Secondary failover	5 days	Tue 11/2/21	Mon 11/8/21
1774	Admin failover	5 days	Tue 11/2/21	Mon 11/8/21
1775	MEVO (optional) failover	5 days	Tue 11/2/21	Mon 11/8/21
1776	**Database operational**	**1 day**	**Tue 11/2/21**	**Tue 11/2/21**
1777	SRDB transitional conversion documented	1 day	Tue 11/2/21	Tue 11/2/21
1778	**RCH toolkit Application**	**21 days**	**Tue 11/2/21**	**Tue 11/30/21**
1779	Tool kit credentials documented	10 days	Tue 11/2/21	Mon 11/15/21
1780	Tool kit RCH setup complete	10 days	Tue 11/16/21	Mon 11/29/21
1781	Tool kit verified	1 day	Tue 11/30/21	Tue 11/30/21
1782	Training	20 days	Tue 6/7/22	Mon 7/4/22
1783	**Carrier Network Conversion**	**111 days**	**Mon 11/15/21**	**Mon 4/18/22**
1784	Phase 1A - LNG & CPE Configuration tasks w/CPE provider	5 days	Mon 11/15/21	Fri 11/19/21
1785	Phase 1B - Confirm CPE Cutover Date	5 days	Mon 1/24/22	Fri 1/28/22
1786	Phase 2 - ESRP Configuration	45 days	Mon 11/22/21	Fri 1/21/22
1787	Phase 3A - Carrier Trunks installed	0 days	Fri 1/21/22	Fri 1/21/22
1788	**Phase 3B - Carrier conversion**	**61 days**	**Mon 1/24/22**	**Mon 4/18/22**
1789	Wireless Conversion	1 day	Mon 1/24/22	Mon 1/24/22

ID	Task Name	Duration	Start	Finish
1790	Wireline Conversion	60 days	Tue 1/25/22	Mon 4/18/22
1791	RCH Closeout Complete	0 days	Mon 7/4/22	Mon 7/4/22
1792	Project Complete	0 days	Mon 7/4/22	Mon 7/4/22

HAMILTON APPENDIX 12: NEBRASKA PROJECT LIFECYCLE TEMPLATE

Hamilton Ne RFP Project Lifecycle

ID	Task Name	Duration	Start	Finish
1	**Project Start**	**458 days**	**Thu 10/1/20**	**Mon 7/4/22**
2	**NGCS**	**458 days**	**Thu 10/1/20**	**Mon 7/4/22**
3	Receive Signed Contract	1 day	Thu 10/1/20	Thu 10/1/20
4	Develop scope of work	1 day	Fri 10/2/20	Fri 10/2/20
5	**Design Phase**	**111 days**	**Fri 10/2/20**	**Fri 3/5/21**
6	**Call Flow questionnaire**	**25 days**	**Fri 10/2/20**	**Thu 11/5/20**
7	Distribute call flow questionnaire to CLIENT on a per site(s) basis	10 days	Fri 10/2/20	Thu 10/15/20
8	Gather and categorize questionnaire results	20 days	Fri 10/9/20	Thu 11/5/20
9	**Site assessment**	**30 days**	**Fri 10/2/20**	**Thu 11/12/20**
10	**Site Survey**	**30 days**	**Fri 10/2/20**	**Thu 11/12/20**
14	**Transport Requirements**	**10 days**	**Fri 11/6/20**	**Thu 11/19/20**
15	SS7 / Sigtran design	10 days	Fri 11/6/20	Thu 11/19/20
16	Carrier trunking Ingress Network design (T1, DS3, OCx)	10 days	Fri 11/6/20	Thu 11/19/20
17	Ethernet (WAN) Network design	10 days	Fri 11/6/20	Thu 11/19/20
18	Commodity Network design	10 days	Fri 11/6/20	Thu 11/19/20
19	**ESInet Requirements**	**15 days**	**Fri 11/13/20**	**Thu 12/3/20**
20	ESInet design completed	15 days	Fri 11/13/20	Thu 12/3/20
21	Circuit Diagrams	15 days	Fri 11/13/20	Thu 12/3/20
22	ESInet design approved	15 days	Fri 11/13/20	Thu 12/3/20
23	**NG Core Network Requirements**	**81 days**	**Fri 11/13/20**	**Fri 3/5/21**
24	**VM Host**	**35 days**	**Fri 11/13/20**	**Thu 12/31/20**
28	**Routers**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
31	**Switches (3650s)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
34	**Local Network Gateway (LNG)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
37	**DACs**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
40	**Monitoring**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
43	**Mevo Server (optional)**	**6 days**	**Fri 11/20/20**	**Fri 11/27/20**
46	**NG ALI Servers (Phase 2)**	**30 days**	**Fri 11/20/20**	**Thu 12/31/20**

Hamilton Ne RFP Project Lifecycle

ID	Task Name	Duration	Start	Finish
49	**Domain Name System (DNS)**	**5 days**	**Fri 11/20/20**	**Thu 11/26/20**
51	**NTP Time Synchronization**	**5 days**	**Fri 11/20/20**	**Thu 11/26/20**
53	**Dial Plan Proxy (DPP)**	**35 days**	**Fri 11/20/20**	**Thu 1/7/21**
56	800 Fail-Over Assignment	5 days	Fri 11/20/20	Thu 11/26/20
57	Common Language Functional Elements (CLFE) Assignment	5 days	Mon 3/1/21	Fri 3/5/21
58	Power / UPS design	5 days	Fri 11/13/20	Thu 11/19/20
59	Physical/Spares	30 days	Fri 11/13/20	Thu 12/24/20
60	**RCH Network Requirements**	**60 days**	**Fri 11/13/20**	**Thu 2/4/21**
61	**Texty design (optional)**	**30 days**	**Fri 11/13/20**	**Thu 12/24/20**
63	**ALI (Local pickup)**	**10 days**	**Fri 12/18/20**	**Thu 12/31/20**
66	**Documentation**	**30 days**	**Fri 12/25/20**	**Thu 2/4/21**
69	**Development Phase**	**186 days**	**Mon 11/23/20**	**Mon 8/9/21**
70	**ESInet**	**132 days**	**Fri 2/5/21**	**Mon 8/9/21**
71	"Providers" Network Availability (driven by priority sheets)	132 days	Fri 2/5/21	Mon 8/9/21
72	**Host Site Hardware**	**70 days**	**Mon 11/23/20**	**Fri 2/26/21**
73	**Data Center A (New)**	**70 days**	**Mon 11/23/20**	**Fri 2/26/21**
111	**Data Center B (Established)**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
119	**Data Center C (Optional)**	**60 days**	**Mon 11/23/20**	**Fri 2/12/21**
127	**Implementation Phase**	**95 days**	**Fri 10/16/20**	**Thu 2/25/21**
128	**Transport**	**95 days**	**Fri 10/16/20**	**Thu 2/25/21**
129	DACs Installation (Data Center A, Data Center B existing)	14 days	Tue 1/12/21	Fri 1/29/21
130	**LNG Installation (Data Center A, Data Center B existing)**	**19 days**	**Tue 1/12/21**	**Fri 2/5/21**
134	Carrier Trunking turned up & tested	51 days	Fri 11/20/20	Fri 1/29/21
135	Router to Router Turned Up & Tested	14 days	Mon 2/8/21	Thu 2/25/21
136	Transfer Codes Confirmed	30 days	Fri 10/16/20	Thu 11/26/20
137	**ESInet**	**201 days**	**Fri 12/4/20**	**Fri 9/10/21**

Hamilton Ne RFP Project Lifecycle

ID	Task Name	Duration	Start	Finish
138	Network Availability	192 days	Fri 12/4/20	Mon 8/30/21
139	Define/configure call logging (NMIS)	14 days	Tue 8/24/21	Fri 9/10/21
140	**Host sites**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
141	**Data Center A**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
142	**NG Core Network**	**49 days**	**Tue 1/12/21**	**Fri 3/19/21**
168	**Data Center B**	**40 days**	**Mon 1/25/21**	**Fri 3/19/21**
169	**NG Core Network**	**40 days**	**Mon 1/25/21**	**Fri 3/19/21**
195	**Region Conversion**	**397 days**	**Fri 12/25/20**	**Mon 7/4/22**
196	**South Central Region**	**309 days**	**Fri 12/25/20**	**Wed 3/2/22**
197	**WAN Testing**	**15 days**	**Mon 3/22/21**	**Fri 4/9/21**
209	**Network Conversion Capability Turn-up**	**111 days**	**Fri 12/25/20**	**Fri 5/28/21**
231	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
246	**Buffalo County Regional Call Host (RCH)**	**208 days**	**Fri 5/7/21**	**Tue 2/22/22**
335	**Dawson County RCH**	**208 days**	**Mon 5/17/21**	**Wed 3/2/22**
424	**South East Region**	**344 days**	**Fri 12/25/20**	**Wed 4/20/22**
425	**WAN Testing**	**15 days**	**Mon 4/12/21**	**Fri 4/30/21**
437	**Network Conversion Capability Turn-up**	**126 days**	**Fri 12/25/20**	**Fri 6/18/21**
459	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
474	**Windstream Data Center (M Street) RCH**	**208 days**	**Fri 6/25/21**	**Tue 4/12/22**
563	**Windstream Data Center (27th Street) RCH**	**208 days**	**Mon 7/5/21**	**Wed 4/20/22**
652	**Metro Region**	**344 days**	**Fri 12/25/20**	**Wed 4/20/22**
653	**WAN Testing**	**15 days**	**Mon 5/3/21**	**Fri 5/21/21**
665	**Network Conversion Capability Turn-up**	**141 days**	**Fri 12/25/20**	**Fri 7/9/21**
687	**OSP Service Conversion**	**100 days**	**Fri 2/5/21**	**Thu 6/24/21**
702	**Douglas County RCH**	**208 days**	**Fri 6/25/21**	**Tue 4/12/22**
791	**Pottawattamie County (IA) RCH**	**208 days**	**Mon 7/5/21**	**Wed 4/20/22**
880	**North Central Region**	**352 days**	**Fri 12/25/20**	**Mon 5/2/22**
881	**WAN Testing**	**15 days**	**Mon 5/24/21**	**Fri 6/11/21**
893	**Network Conversion Capability Turn-up**	**156 days**	**Fri 12/25/20**	**Fri 7/30/21**
915	**OSP Service Conversion**	**108 days**	**Fri 2/5/21**	**Tue 7/6/21**

Hamilton Ne RFP Project Lifecycle

ID	Task Name	Duration	Start	Finish
930	**Boyd/Holt RCH**	**208 days**	**Wed 7/7/21**	**Fri 4/22/22**
1019	**Cherry County RCH**	**208 days**	**Thu 7/15/21**	**Mon 5/2/22**
1108	**East Central Region**	**367 days**	**Fri 12/25/20**	**Mon 5/23/22**
1109	**WAN Testing**	**15 days**	**Mon 6/14/21**	**Fri 7/2/21**
1121	**Network Conversion Capability Turn-up**	**171 days**	**Fri 12/25/20**	**Fri 8/20/21**
1143	**OSP Service Conversion**	**123 days**	**Fri 2/5/21**	**Tue 7/27/21**
1158	**City of Columbus RCH**	**208 days**	**Wed 7/28/21**	**Fri 5/13/22**
1247	**Saunders County RCH**	**208 days**	**Thu 8/5/21**	**Mon 5/23/22**
1336	**North East Region (in development)**	**382 days**	**Fri 12/25/20**	**Mon 6/13/22**
1337	**WAN Testing**	**15 days**	**Mon 7/5/21**	**Fri 7/23/21**
1349	**Network Conversion Capability Turn-up**	**186 days**	**Fri 12/25/20**	**Fri 9/10/21**
1371	**OSP Service Conversion**	**138 days**	**Fri 2/5/21**	**Tue 8/17/21**
1386	**Norfolk RCH**	**208 days**	**Wed 8/18/21**	**Fri 6/3/22**
1475	**South Sioux City RCH**	**208 days**	**Thu 8/26/21**	**Mon 6/13/22**
1564	**Metro West Region (in development)**	**397 days**	**Fri 12/25/20**	**Mon 7/4/22**
1565	**WAN Testing**	**15 days**	**Mon 7/26/21**	**Fri 8/13/21**
1577	**Network Conversion Capability Turn-up**	**201 days**	**Fri 12/25/20**	**Fri 10/1/21**
1599	**OSP Service Conversion**	**153 days**	**Fri 2/5/21**	**Tue 9/7/21**
1614	**Fremont/Dodge County 911 RCH**	**208 days**	**Wed 9/8/21**	**Fri 6/24/22**
1703	**Colfax County 911 RCH**	**208 days**	**Thu 9/16/21**	**Mon 7/4/22**
1792	Project Complete	0 days	Mon 7/4/22	Mon 7/4/22

HAMILTON APPENDIX 13: TRAINEE CHECKLIST — STATE OF NEBRASKA

Trainee Checklist – State of Nebraska

Name: _____ Location: _____ Staff ID #: _____

*Please review the following checklist and indicate if you have **practiced** each call type and procedure. Subjects with an (*) indicates topics that were presented by either the Trainer or an employee of Hamilton.*

NE911.net

NOC / SOC Procedures	Yes ☐	No ☐
Escalations	Yes ☐	No ☐
Trouble Reporting	Yes ☐	No ☐
Help Desk Portal	Yes ☐	No ☐

Date: _____

Toolkit

Maintenance Interface	Yes ☐	No ☐
Basic MIS	Yes ☐	No ☐

Date: _____

911 Logix

Executive Dashboard	Yes ☐	No ☐
Advanced MIS	Yes ☐	No ☐
Buttons	Yes ☐	No ☐
Running Reports	Yes ☐	No ☐
Research Event Impacts	Yes ☐	No ☐

Date: _____

MEVO(+)

Back-up to CPE	Yes ☐	No ☐
Disaster Recovery – Anywhere Kit	Yes ☐	No ☐
Buttons	Yes ☐	No ☐
Call Capabilities	Yes ☐	No ☐
Real-Time Text	Yes ☐	No ☐
ANI / ALI	Yes ☐	No ☐
Other Message Solutions	Yes ☐	No ☐

Date: _____

Texty

Dashboard	Yes ☐	No ☐
Inbound & Outbound Text	Yes ☐	No ☐
Push to CAD	Yes ☐	No ☐
Transfer & Barge	Yes ☐	No ☐
Language Interpretation	Yes ☐	No ☐
Map	Yes ☐	No ☐

Date: _____

HAMILTON APPENDIX 14: SAMPLE MEVO(+) TRAINING OUTLINE

MEVO(+) Training Outline

TRAINER: Hamilton NG911, Inc.
LOCATION: [fill in here]
DURATION: 3 hours

☐ Introduction:

- ☐ Standard trainer / trainee intros; enabling access, logins, etc.

Training Expectations:

- ☐ What you can expect from us: three hours classroom and/or online training, quality standard requirements, positive and corrective feedback and coaching support. What we expect from you: Reliable attendance and active engagement; be present, on time, and focused on training tasks.
- ☐ Conduct: Respond to your learning process with self-compassion. Remain receptive and open to all that the full training experience offers, and our feedback/coaching. Respond to errors with resiliency. Training might be casual/fun at times but maintain professionalism.

☐ Buttons:

- ☐ High-level rundown of features and capabilities
- ☐ Hard keys and functions
- ☐ Touchscreen icons and components
- ☐ Customization
- ☐ Settings

☐ Call Capabilities:

- ☐ Call capabilities rundown
- ☐ Placing and ending calls
- ☐ Answering calls
- ☐ Ignoring, silencing, and redialing calls
- ☐ Redial call history
- ☐ Muting capabilities
- ☐ Hold and resume a call
- ☐ 9-1-1 transfer
- ☐ Barge, rebid and call back
- ☐ Conference call
- ☐ Non-Service Initialized (NSI)
- ☐ 9-1-1 call history
- ☐ All call history
- ☐ IRR-Recorder
- ☐ Video examples / demos

☐ 10-Minute Break

☐ **ANI / ALI:**

- ☐ Spill-wireline
- ☐ Spill wireless
- ☐ Mapping features
- ☐ 9-1-1 details screen
- ☐ Video examples / demos

☐ **Real-Time Text (RTT):**

- ☐ Incoming RTT calls
- ☐ RTT screen interface
- ☐ RTT with mapping
- ☐ Video examples / demos

☐ **Other Message Solutions:**

- ☐ Incoming SMS
- ☐ Incoming MMS
- ☐ Message solutions with mapping interface
- ☐ Video examples / demos

☐ **10-Minute Break**

☐ **Disaster Recovery – Anywhere Kit:**

- ☐ 4G VPN connectivity
- ☐ Platform rundown
- ☐ Continuity of operations (COOP)
- ☐ Situational simulation
- ☐ Video examples / demos

☐ **Back-up to CPE**

- ☐ Call redirection (per NOC/SOC)
- ☐ Separate VoIP workstation
- ☐ Situational simulation
- ☐ Video examples / demos

☐ **Additional Questions**

☐ **Wrap-Up**

- ☐ Trainee checklist sheets
- ☐ Shut Down/Clean Up Procedure
- ☐ Equipment Storage

HAMILTON APPENDIX 15: HAMILTON TRAINING MATERIALS

911Logix Training

Hamilton NG911
www.HamiltonNG911.com
NG911@hamiltontel.com
800.821.1831

HAMILTON NG911

Agenda

- How to Access 911Logix
- Buttons
- Reports

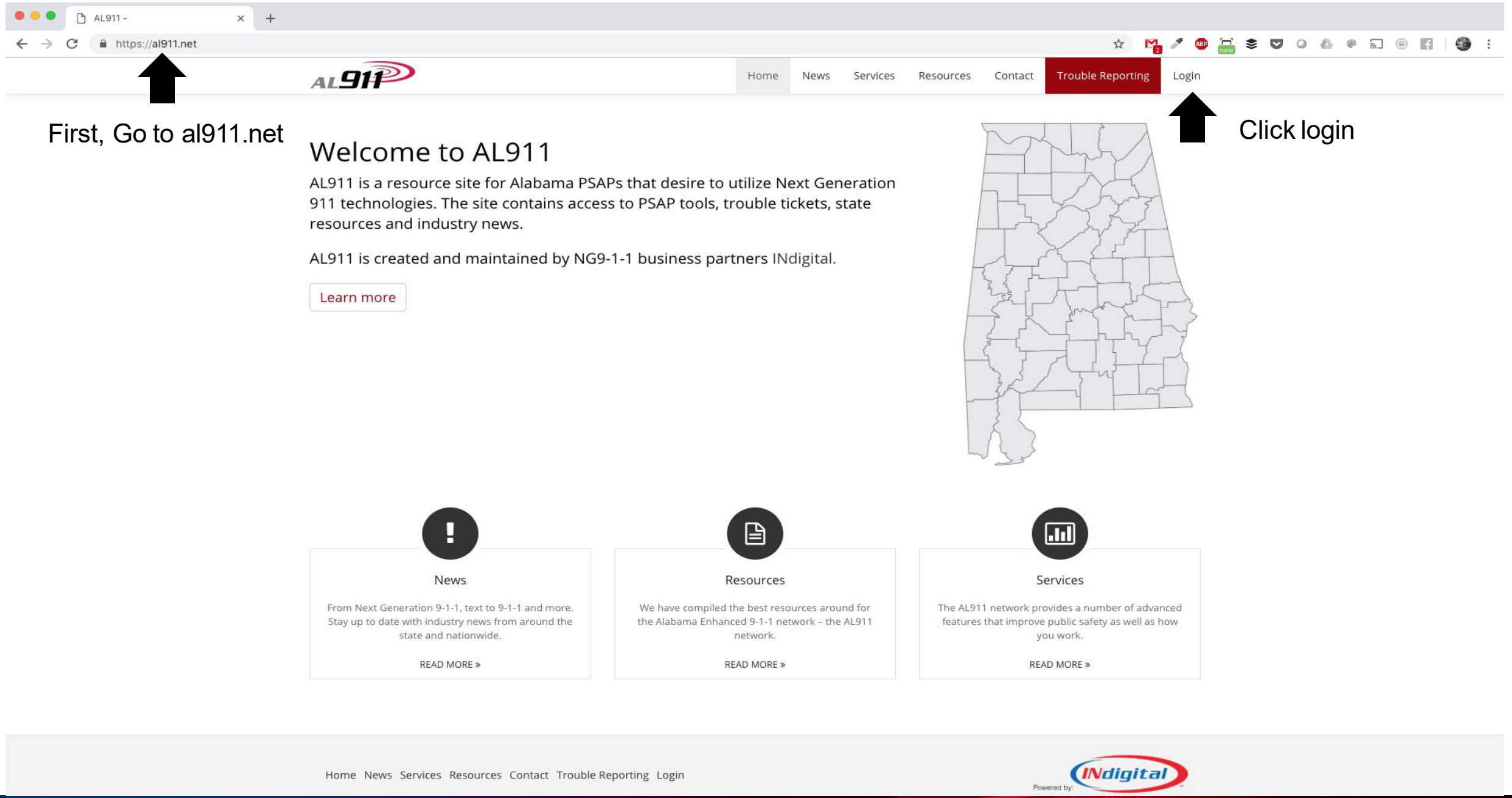
911Logix

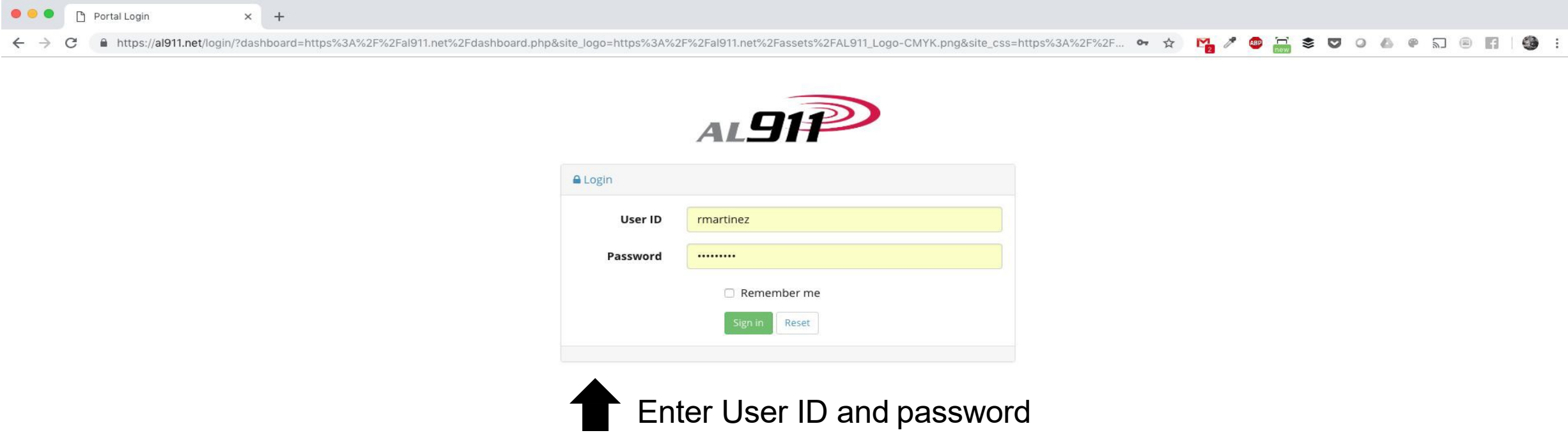
How to Access

HAMILTON NG911

First, Go to al911.net

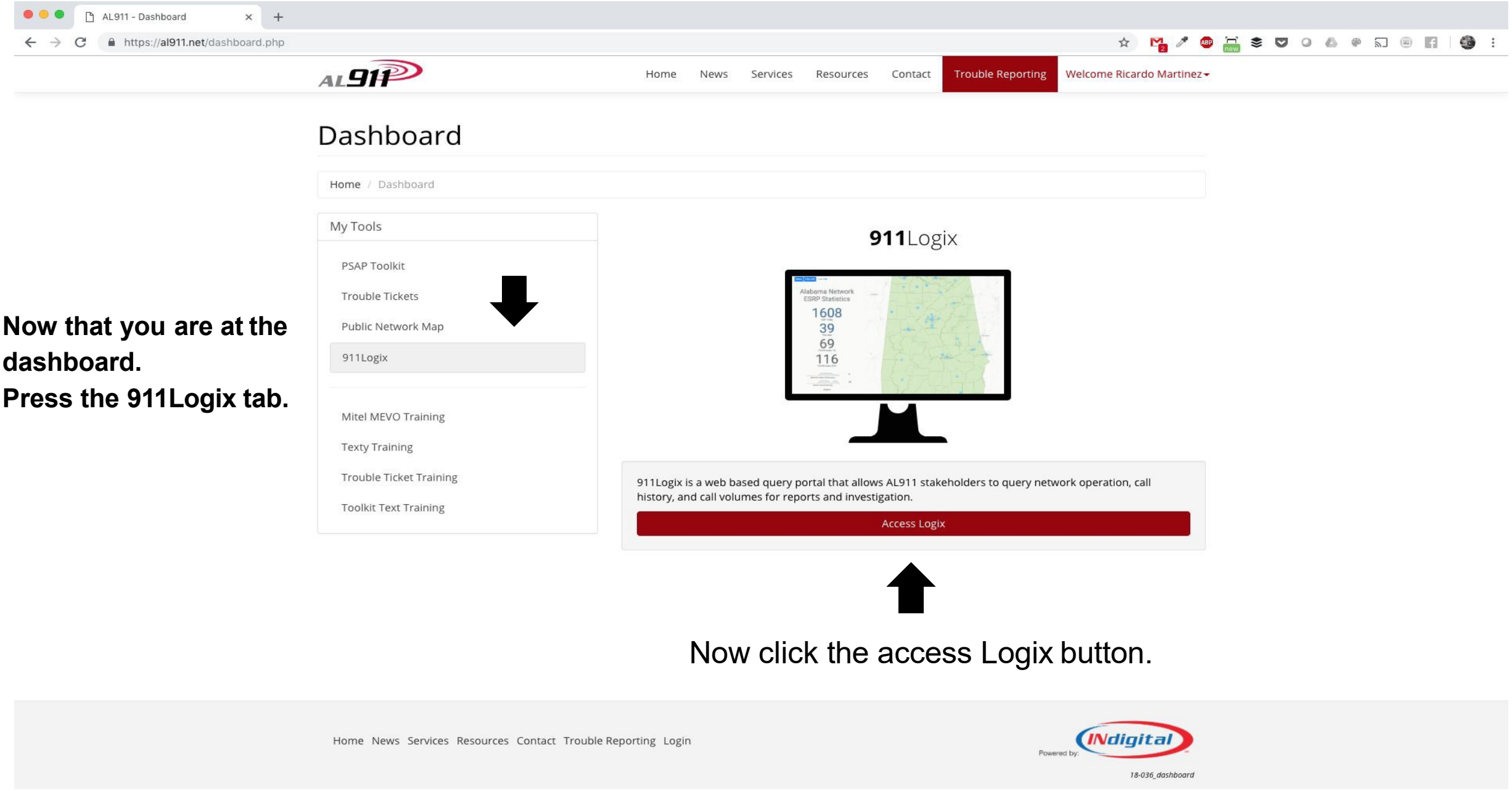
Click login



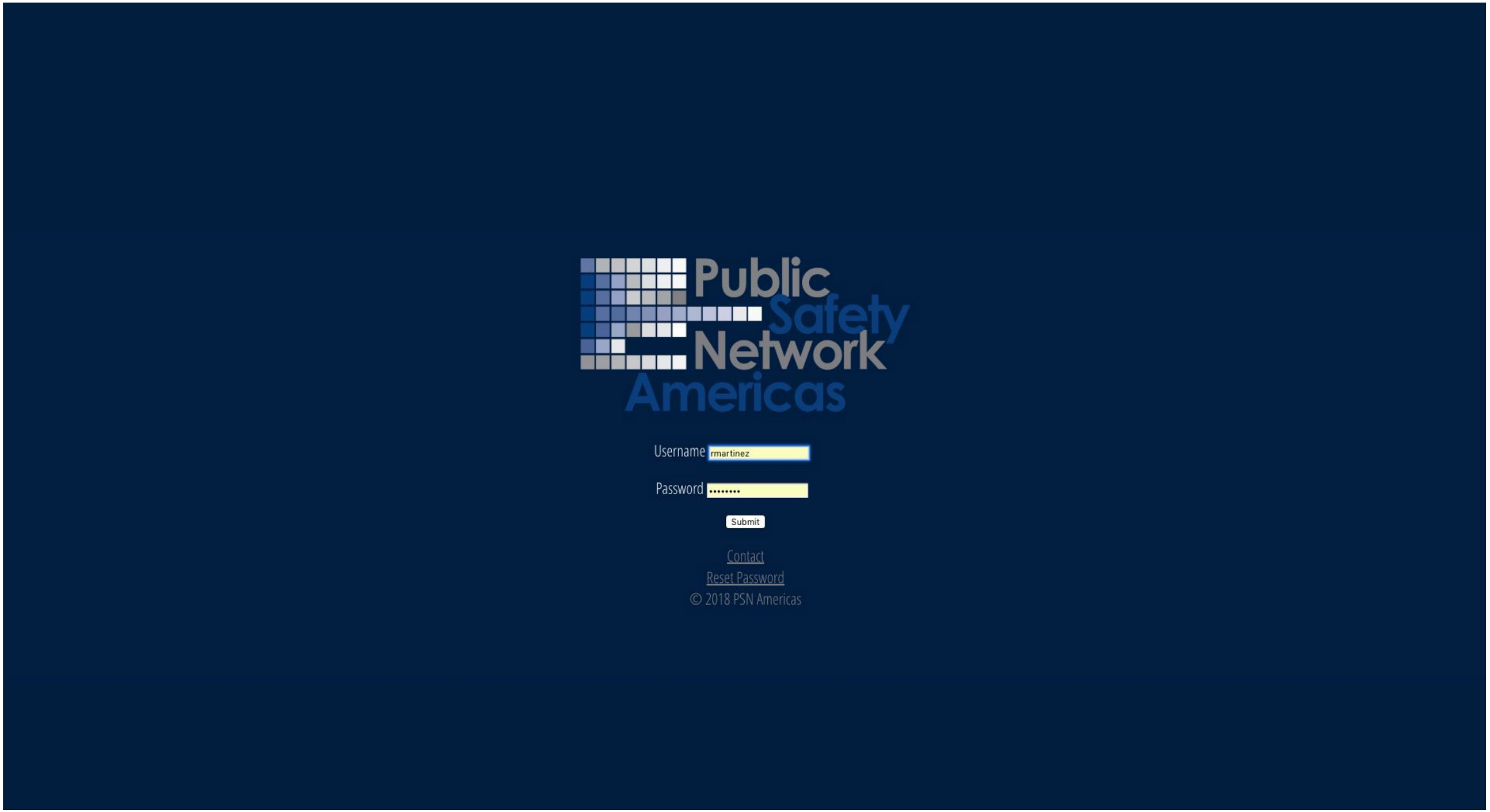


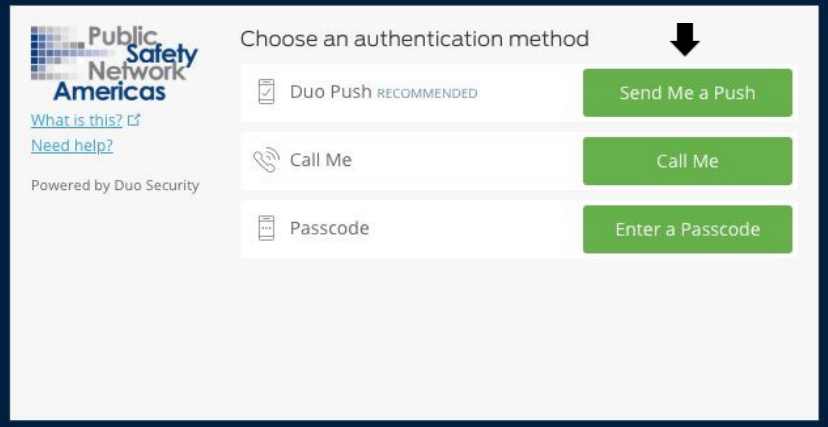
Enter User ID and password

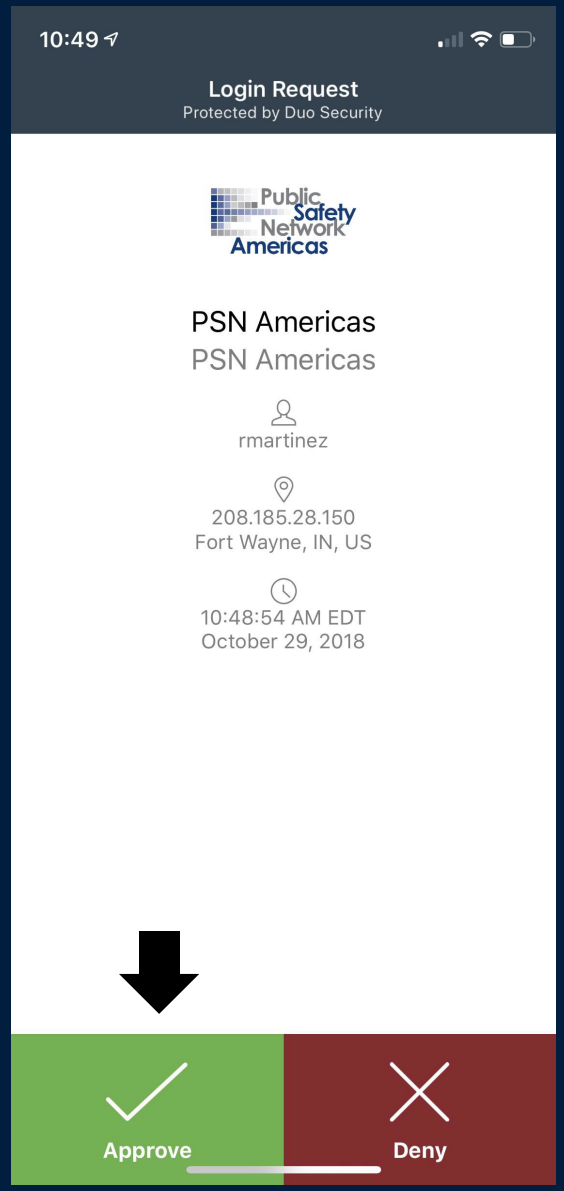
Now that you are at the dashboard.
Press the 911Logix tab.



Now click the access Logix button.

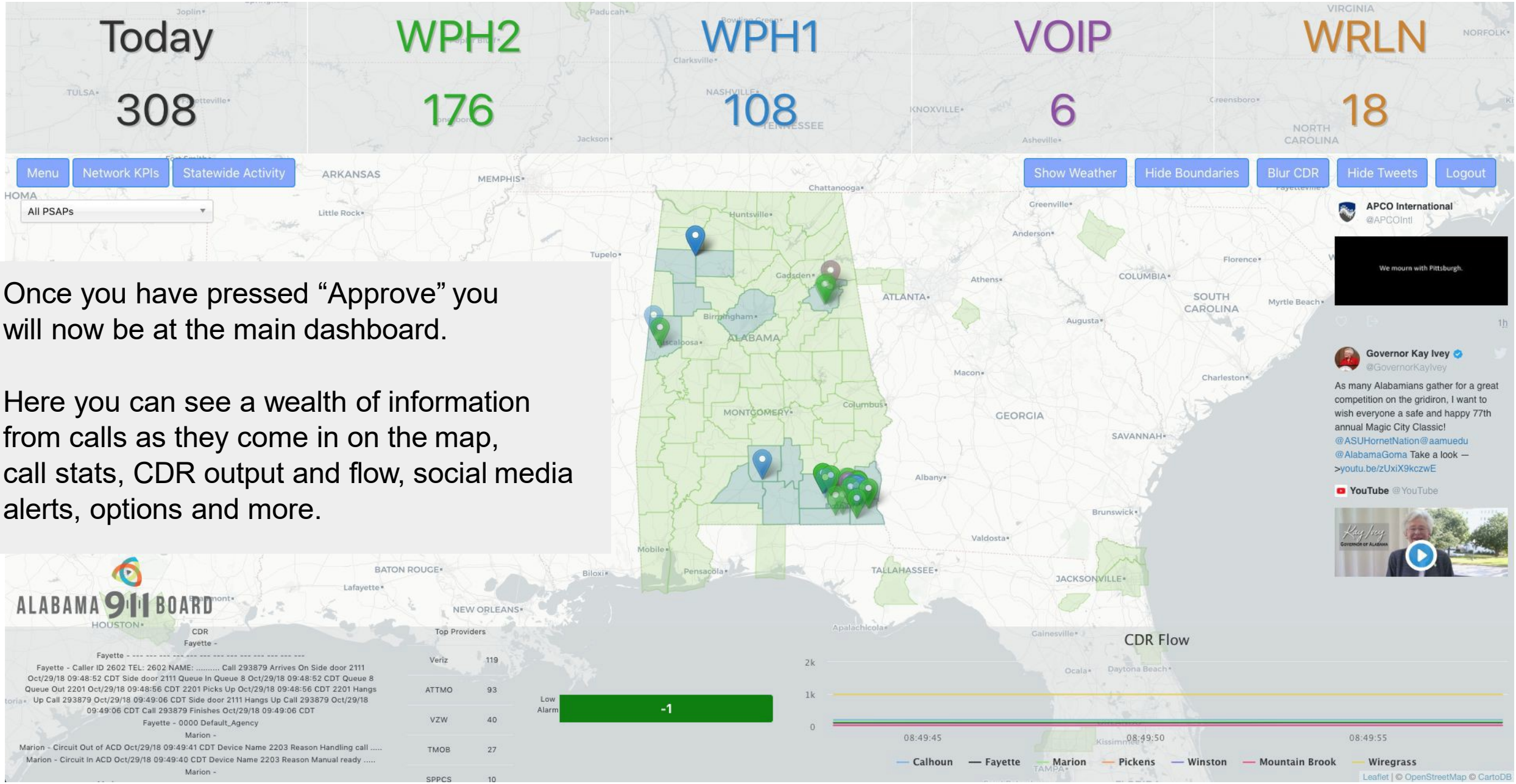






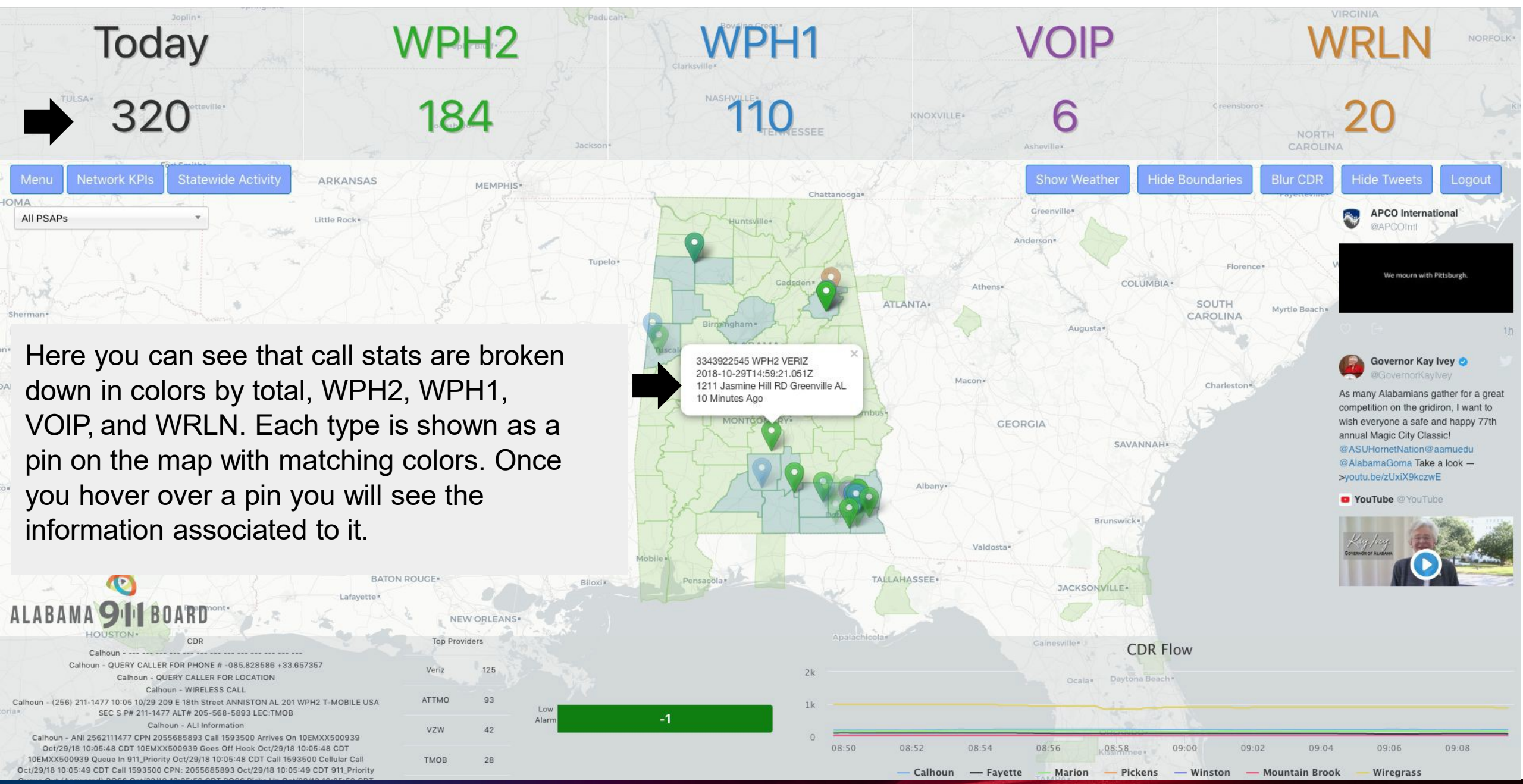
Once you have typed in your username and password you will see the two factor authentication options. If you choose a Duo Push you will be prompted with the following on your phone.

Press “Approve”



Once you have pressed “Approve” you will now be at the main dashboard.

Here you can see a wealth of information from calls as they come in on the map, call stats, CDR output and flow, social media alerts, options and more.

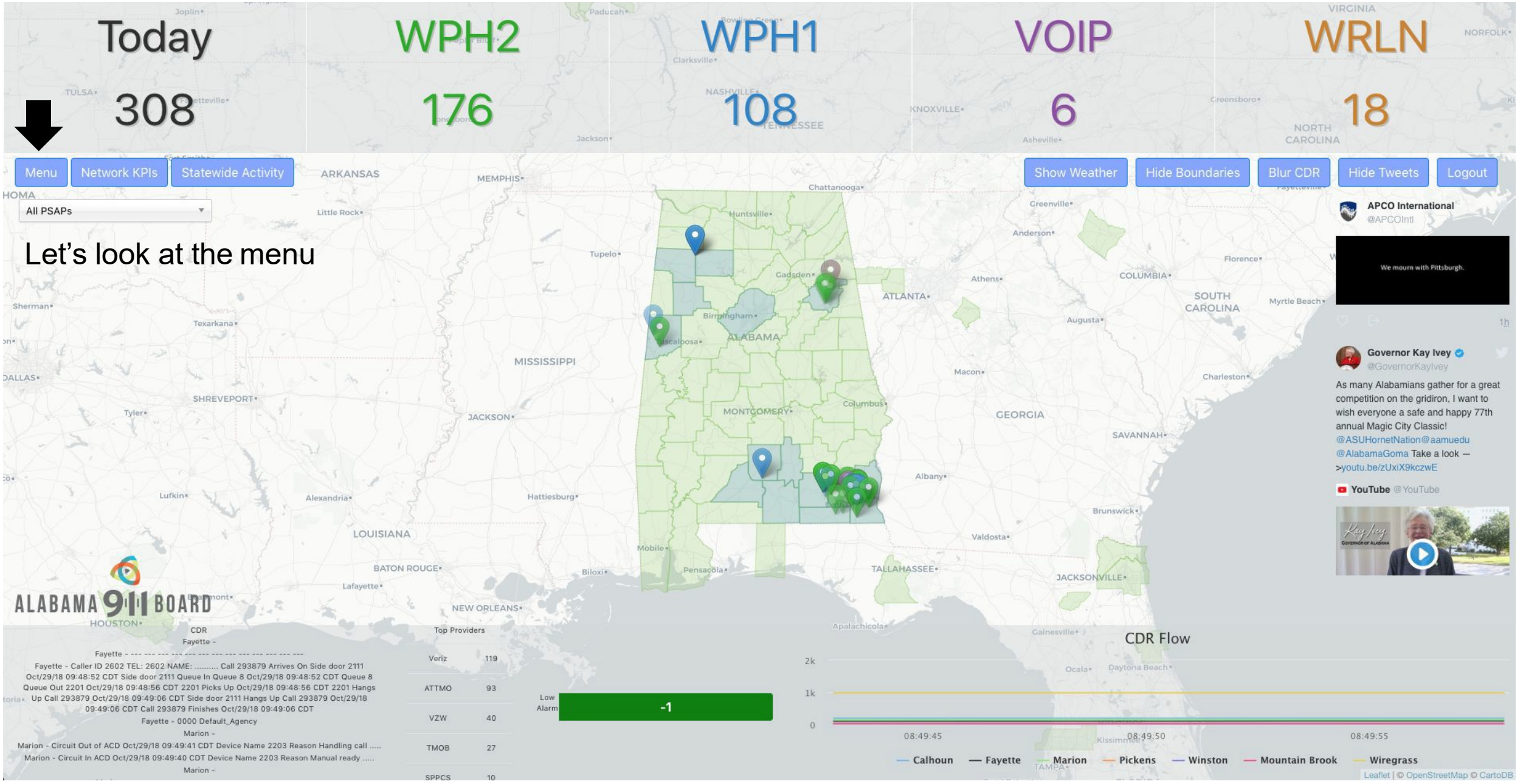


HAMILTON NG911

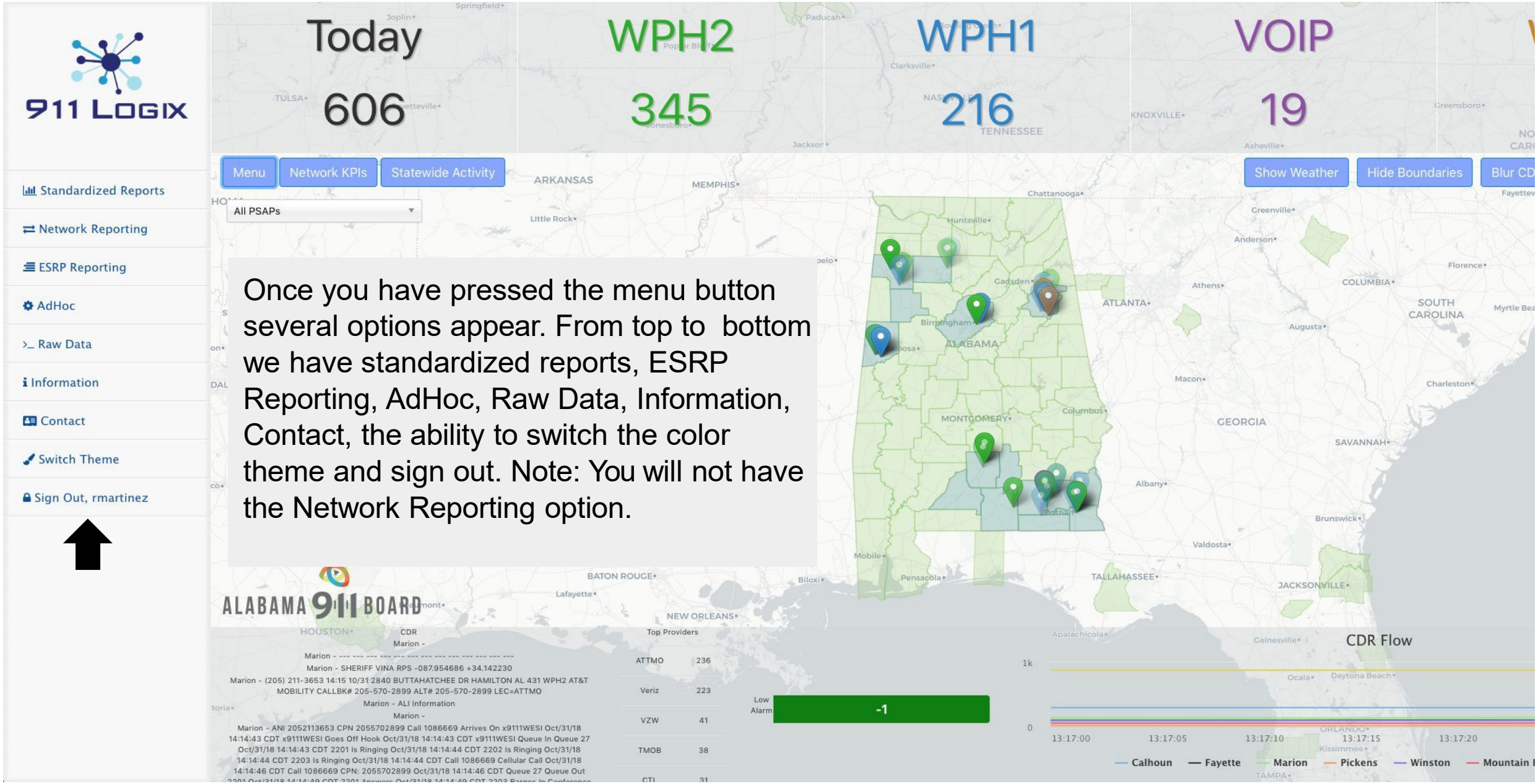
911Logix

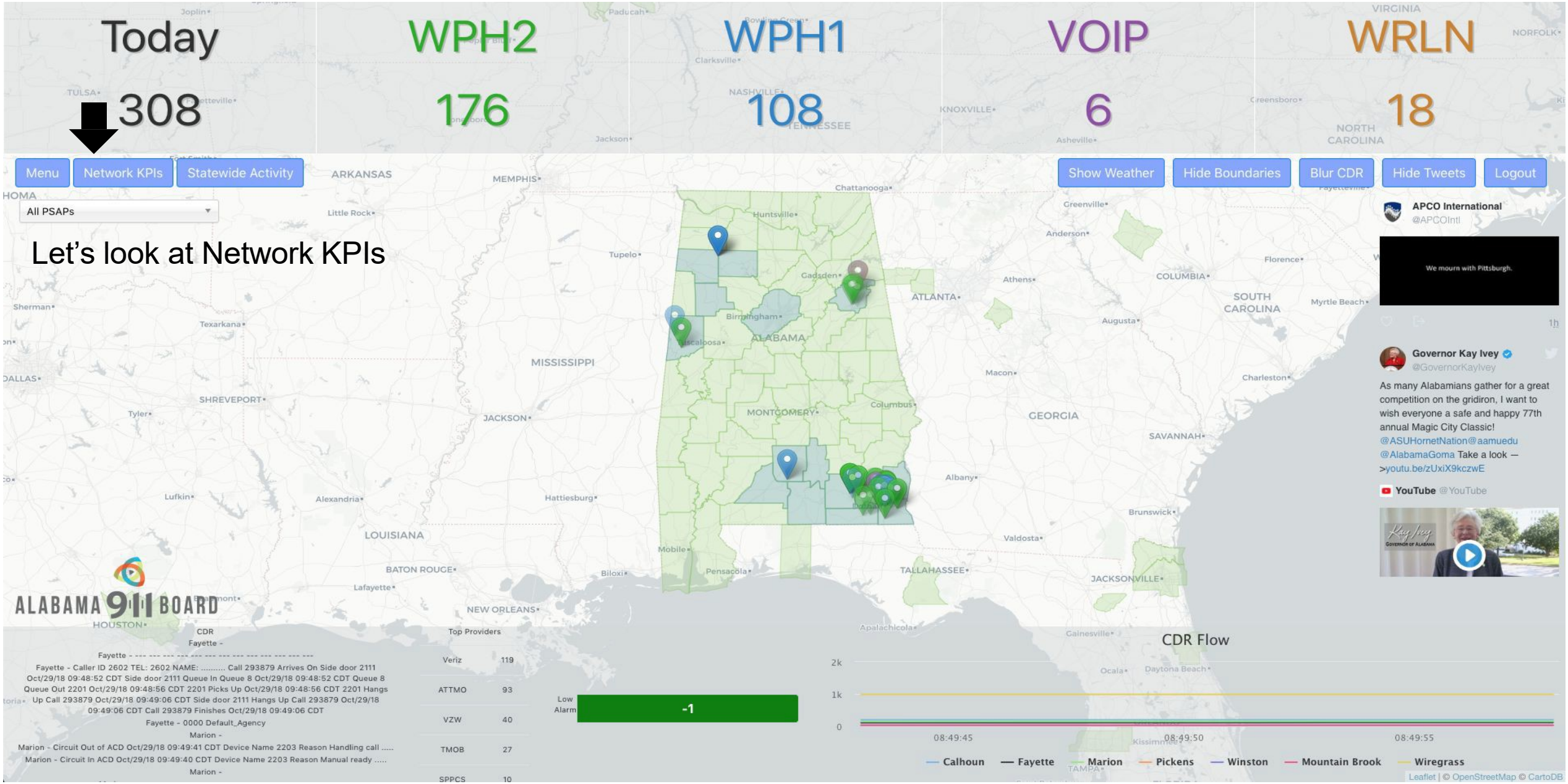
Buttons

HAMILTON NG911



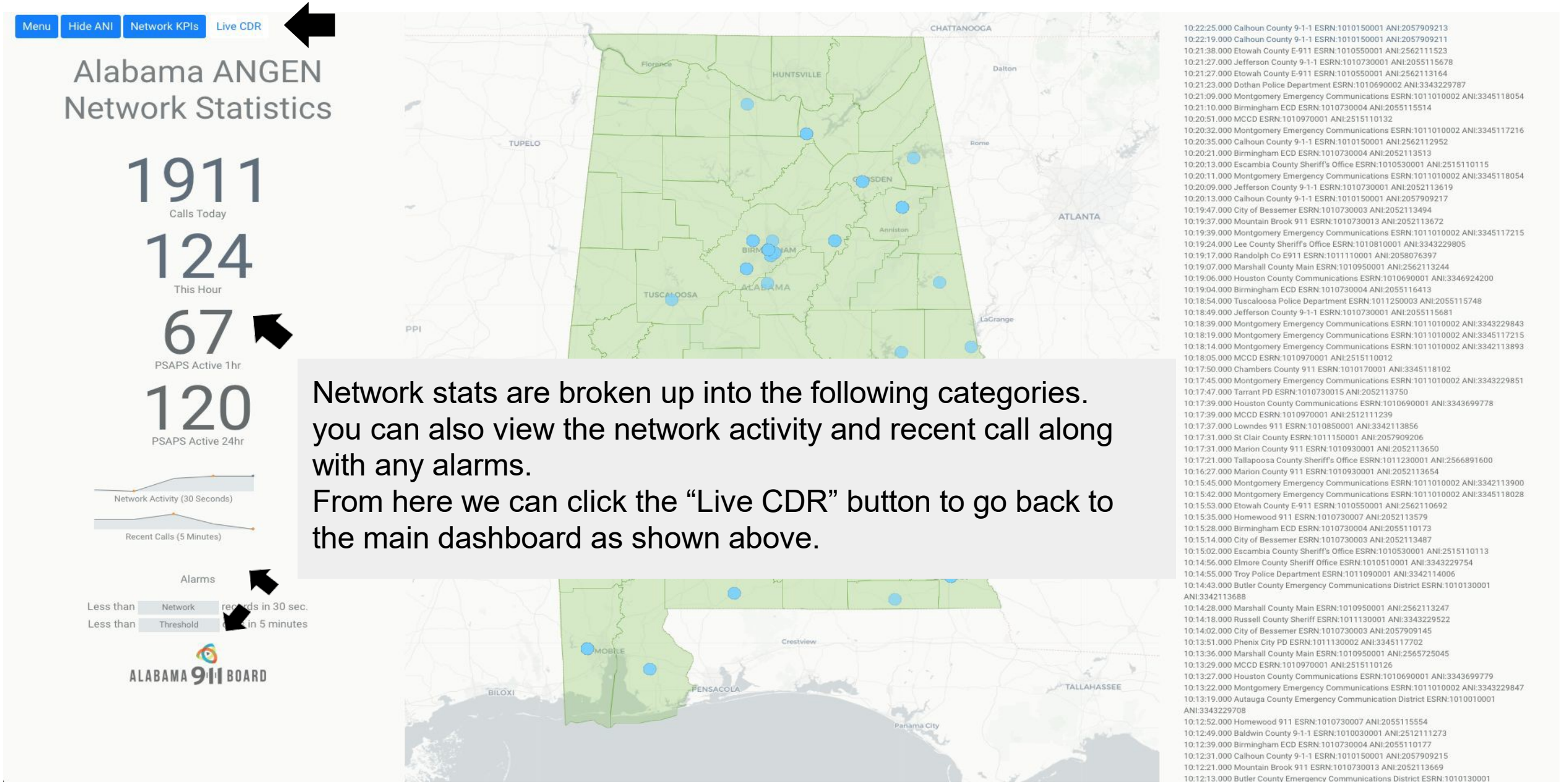
HAMILTON NG911





The next button is the statewide activity dashboard which can be accessed from the Network KPI dashboard.

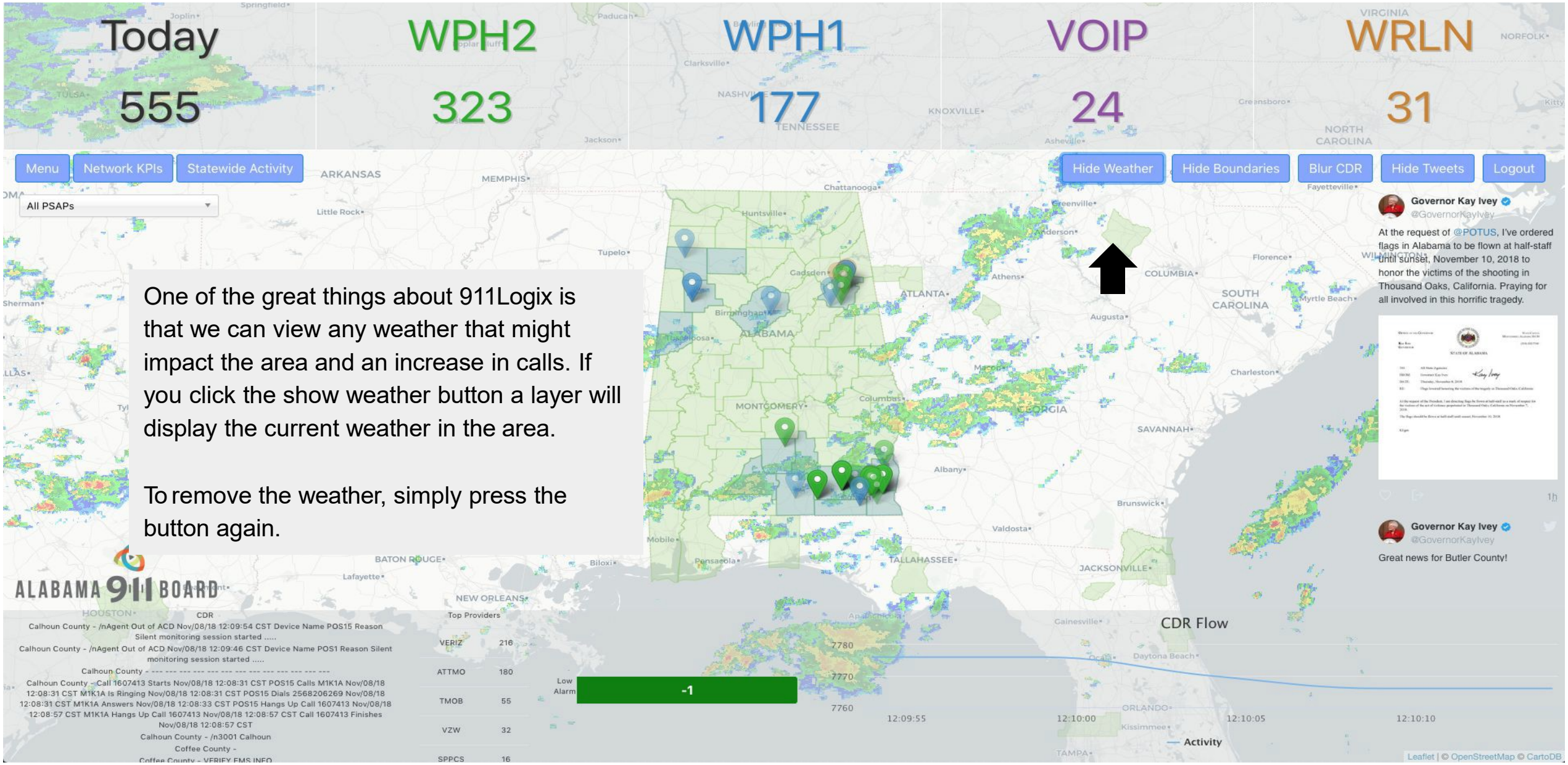
Network KPIs (Key Performance Indicators) are split up in different categories for your center.

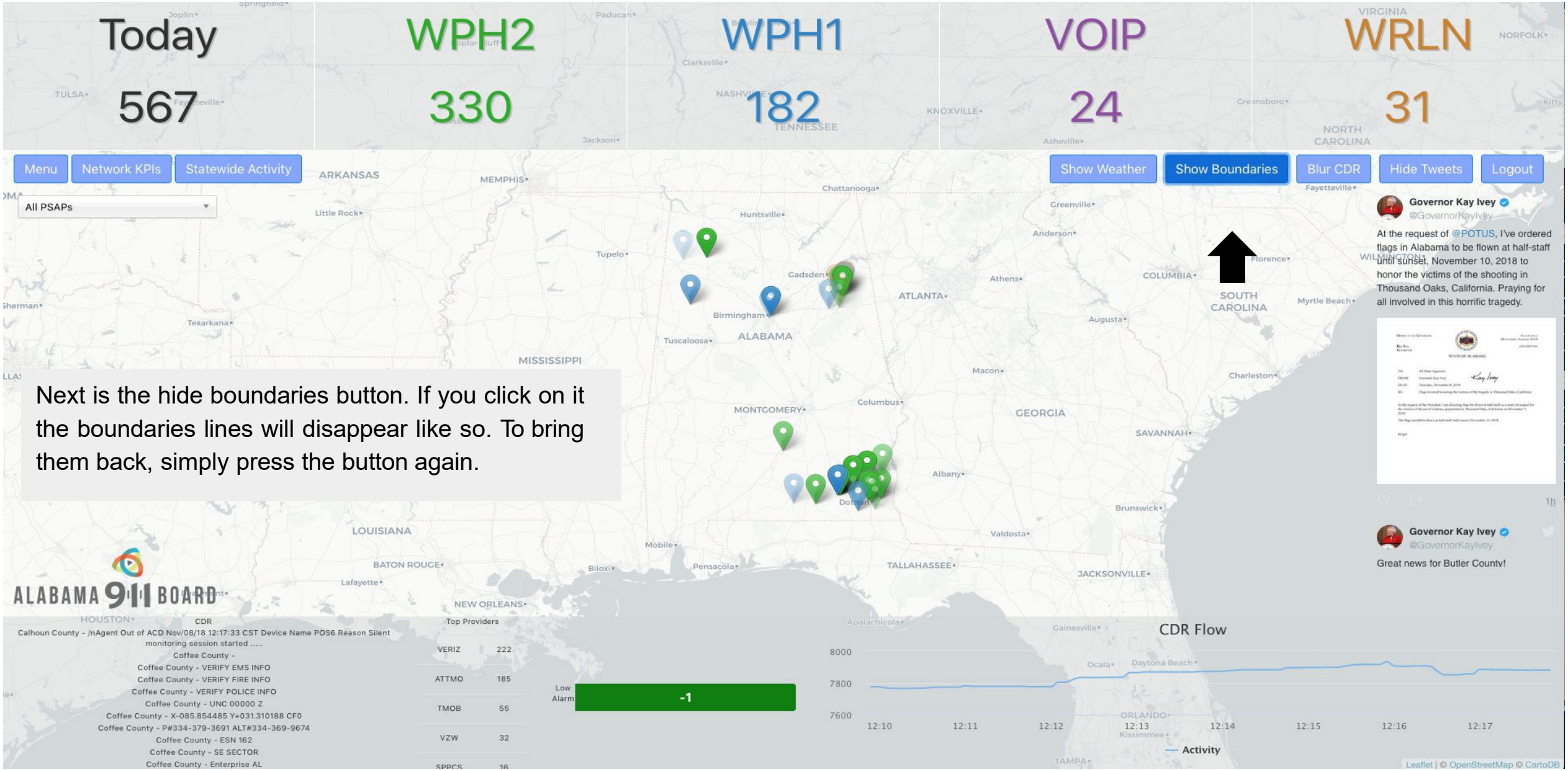


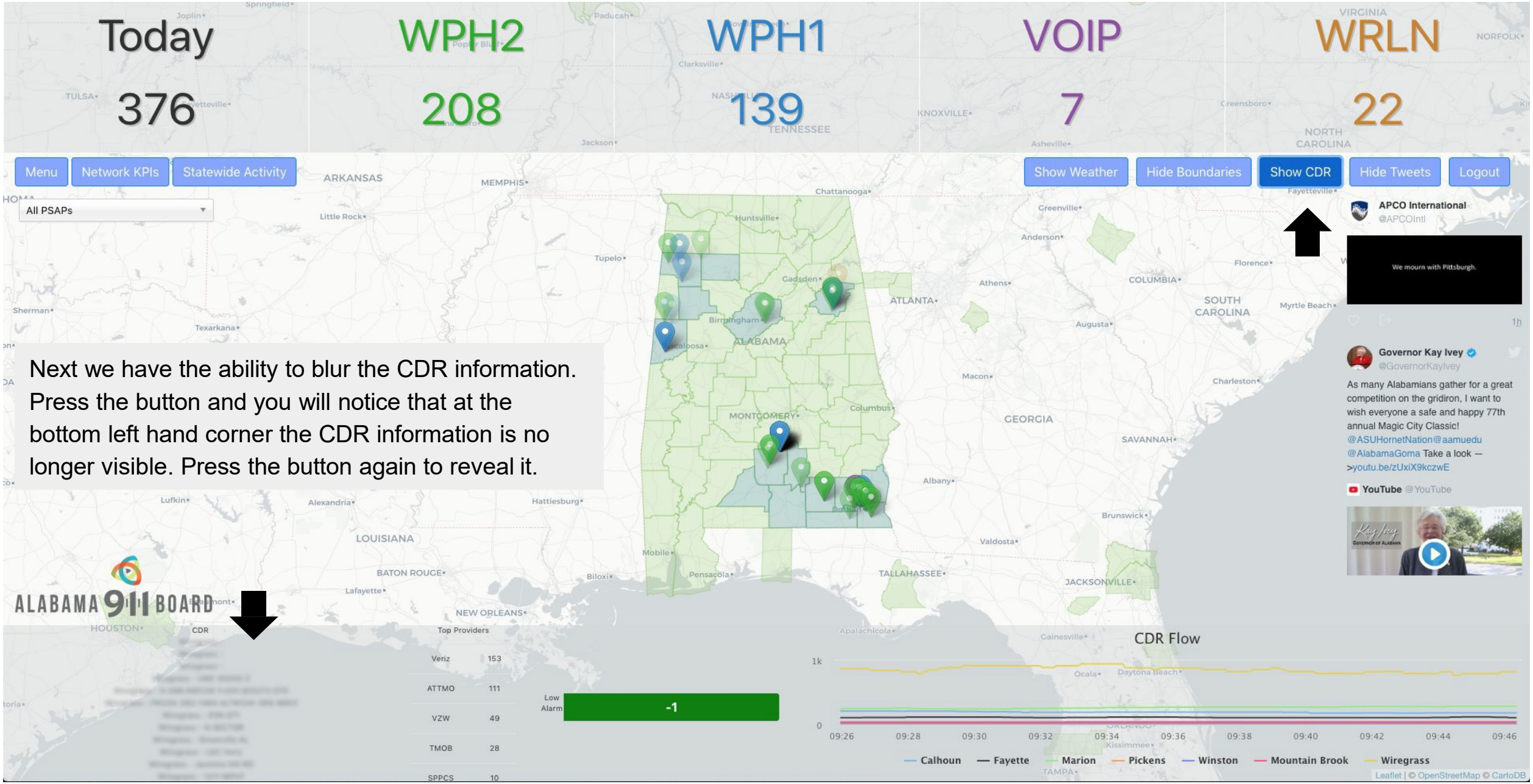
Network stats are broken up into the following categories. you can also view the network activity and recent call along with any alarms.

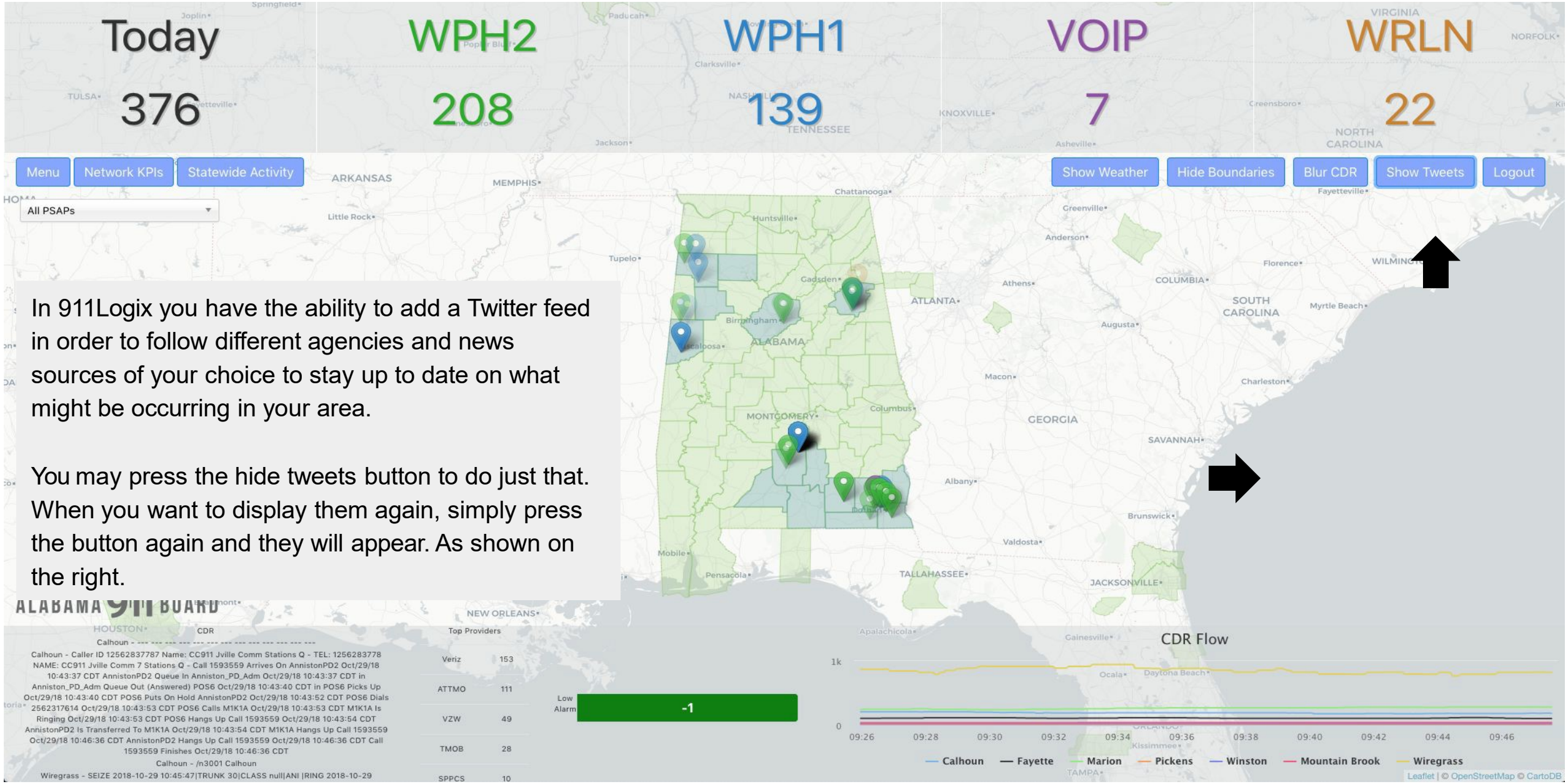
From here we can click the “Live CDR” button to go back to the main dashboard as shown above.

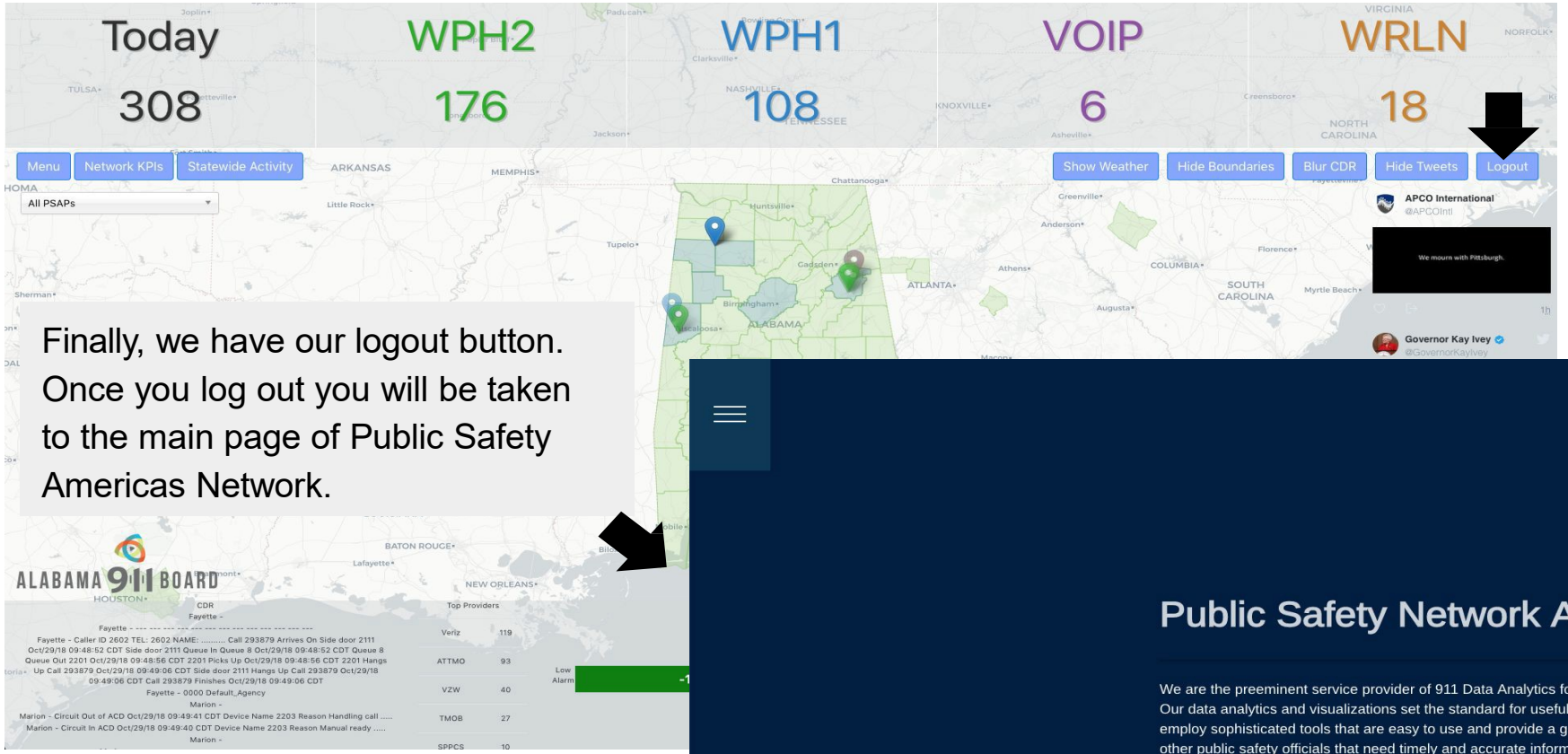
HAMILTON NG911







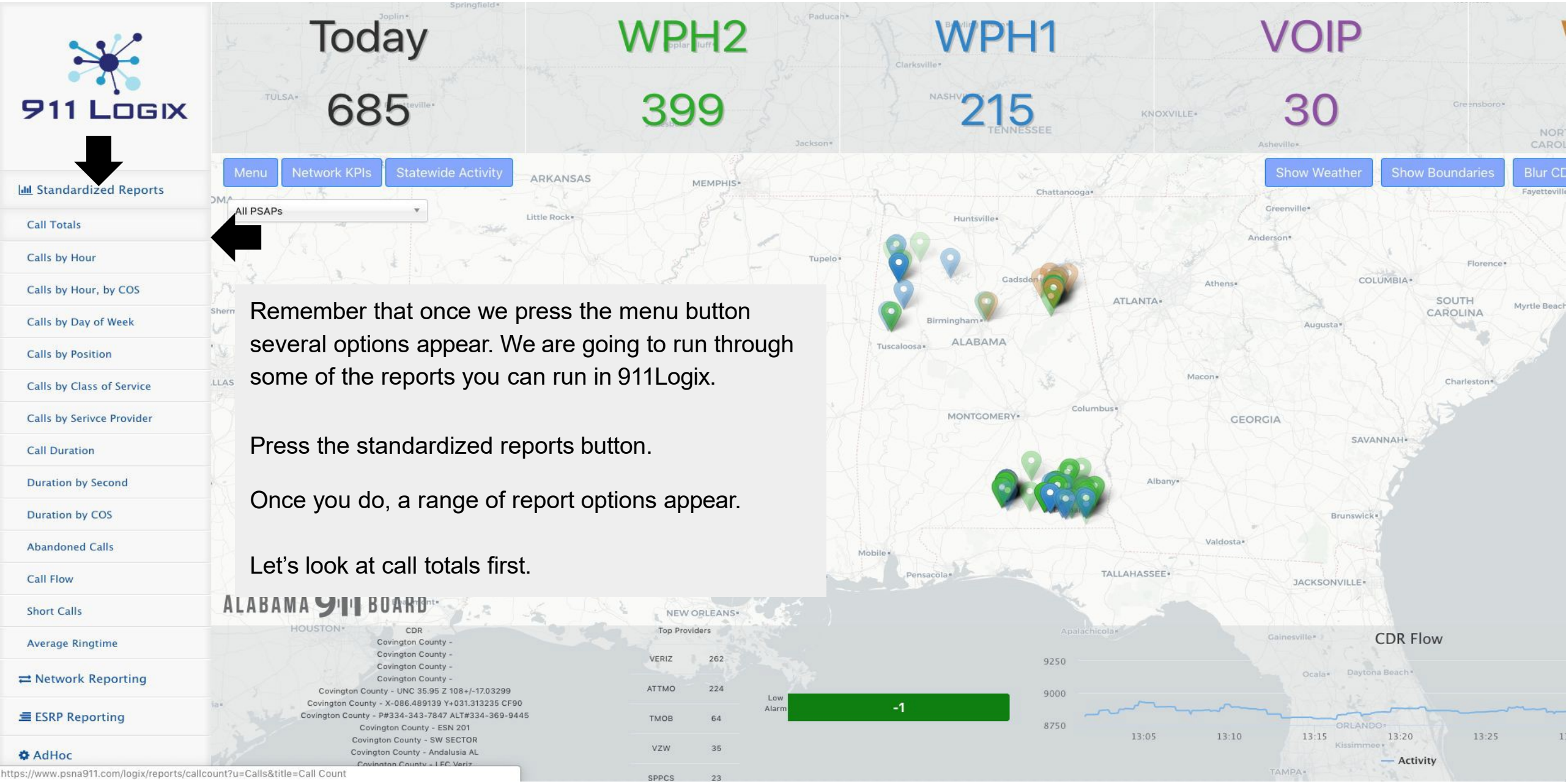


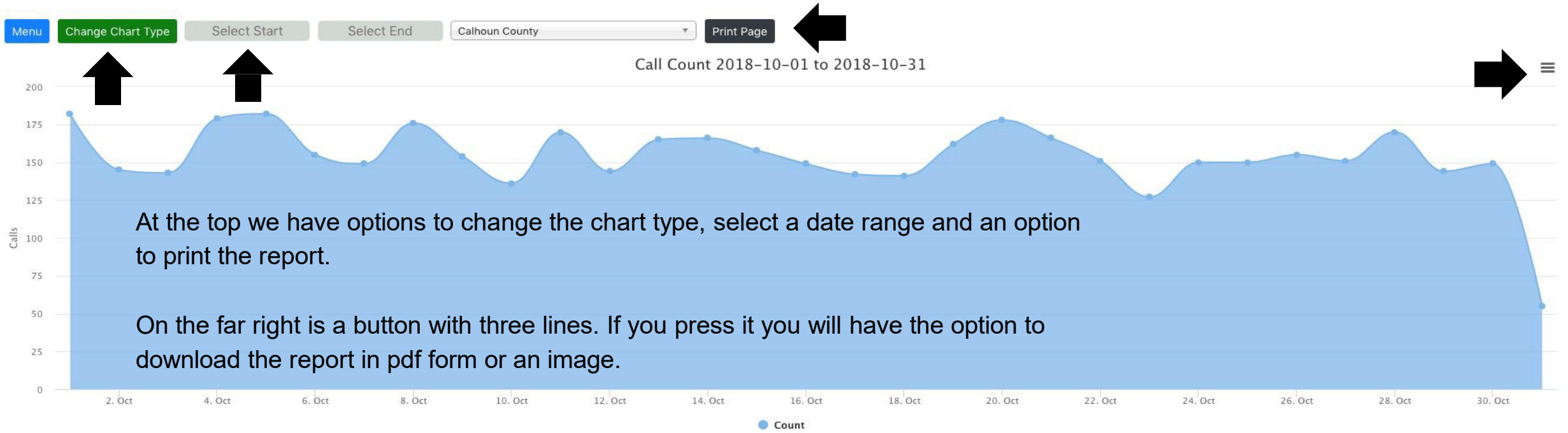


Finally, we have our logout button. Once you log out you will be taken to the main page of Public Safety Americas Network.

911Logix

Reports





At the top we have options to change the chart type, select a date range and an option to print the report.

On the far right is a button with three lines. If you press it you will have the option to download the report in pdf form or an image.

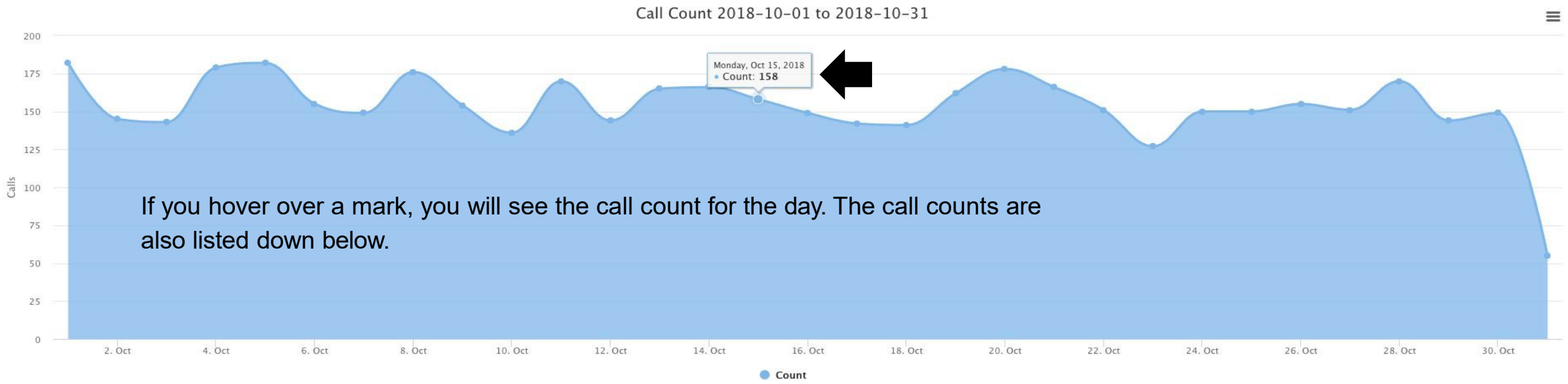
Copy CSV PDF

Search:

Average	153.03
Totals	4744 (100.0%)

Date	Count
2018-10-01	182
2018-10-02	145
2018-10-03	143
2018-10-04	179
2018-10-05	182
2018-10-06	155
2018-10-07	149

Menu | Change Chart Type | Select Start | Select End | Calhoun County | Print Page



Copy | CSV | PDF

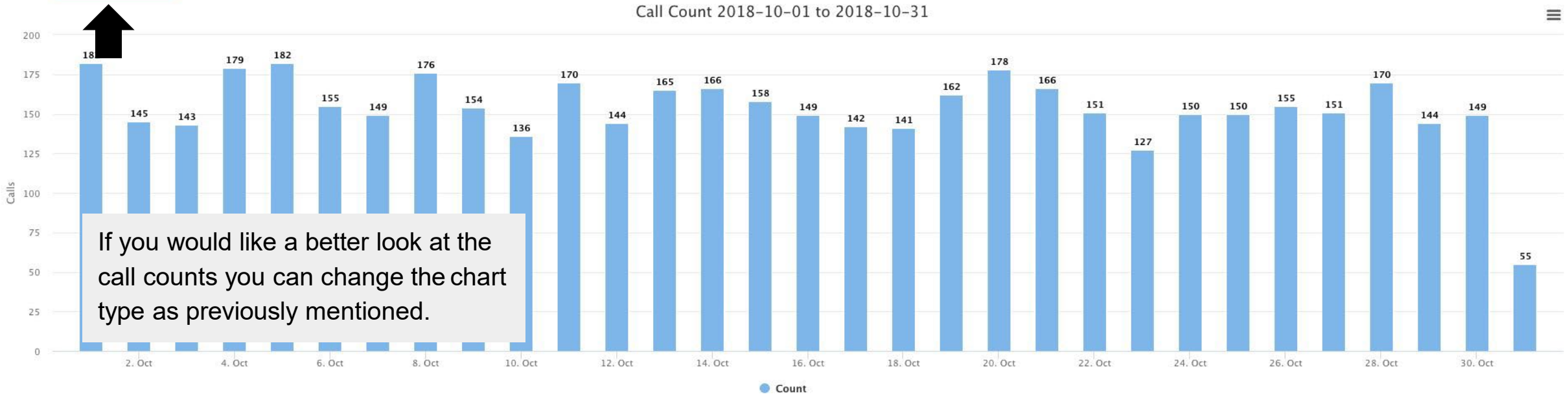
Search:

Average	153.03
Totals	4744 (100.0%)

Date	Count
2018-10-01	182
2018-10-02	145
2018-10-03	143
2018-10-04	179
2018-10-05	182
2018-10-06	155
2018-10-07	149
2018-10-08	176

HAMILTON NG911

Menu | Change Chart Type | Select Start | Select End | Calhoun County | Print Page



If you would like a better look at the call counts you can change the chart type as previously mentioned.

Copy CSV PDF

Search:

Average	153.03
Totals	4744 (100.0%)

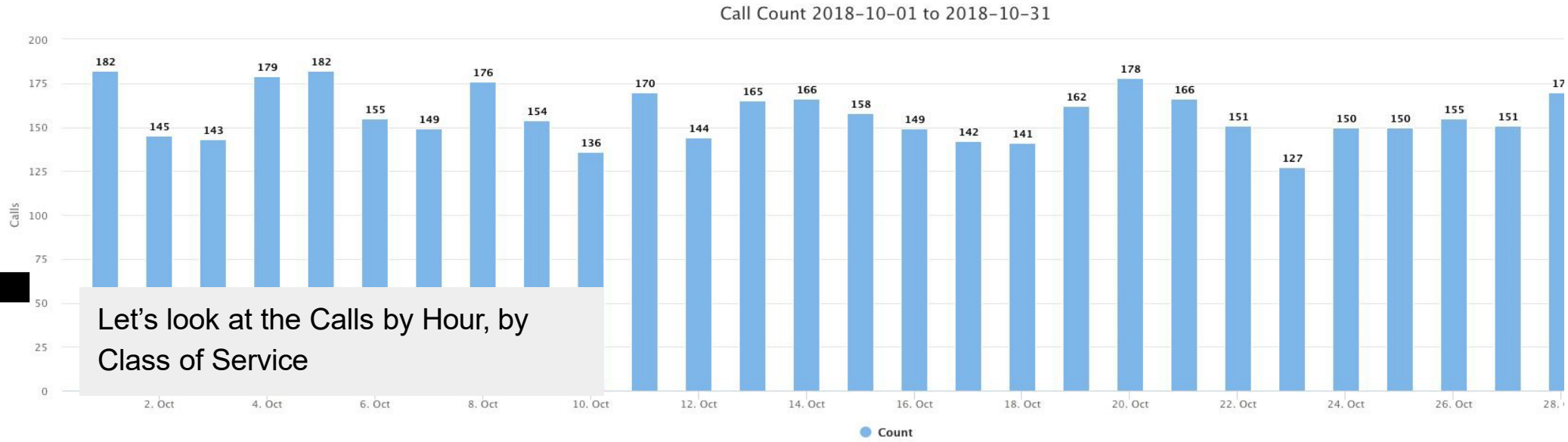
Date	Count
2018-10-01	182
2018-10-02	145
2018-10-03	143
2018-10-04	179
2018-10-05	182
2018-10-06	155
2018-10-07	149

HAMILTON NG911

911 Logix

- Standardized Reports
  - Call Totals
  - Calls by Hour
  - Calls by Hour, by COS
  - Calls by Day of Week
  - Calls by Position
  - Calls by Class of Service
  - Calls by Serivce Provider
  - Call Duration
  - Duration by Second
  - Duration by COS
  - Abandoned Calls
  - Call Flow
  - Short Calls
  - Average Ringtime
- Network Reporting
- ESRP Reporting
- AdHoc

Menu | Change Chart Type | Select Start | Select End | Calhoun County | Print Page



Let's look at the Calls by Hour, by Class of Service

Copy | CSV | PDF

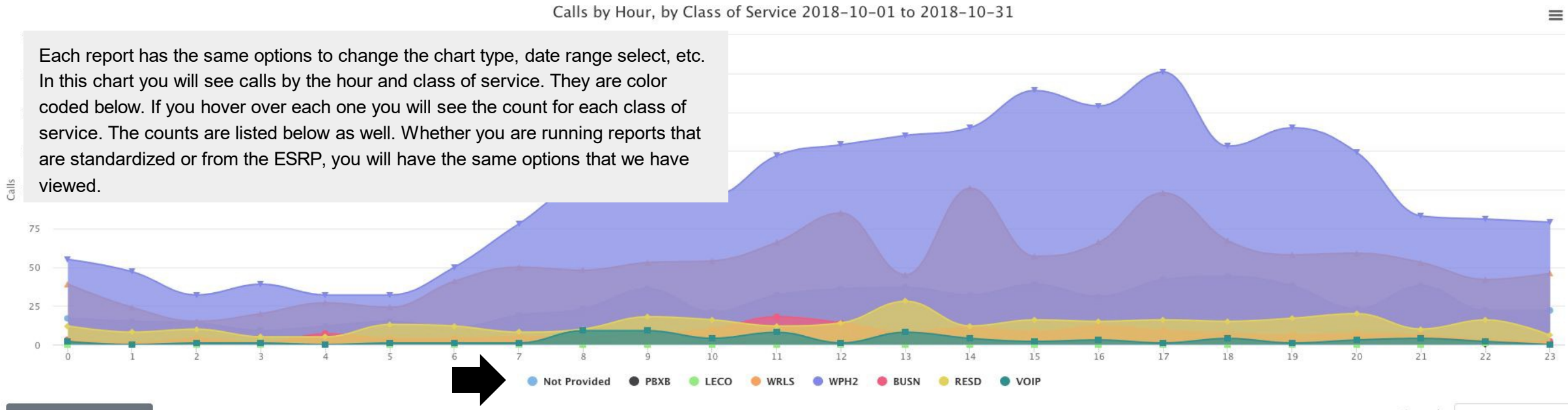
Average	153.03
Totals	4744 (100.0%)

Date	Count
2018-10-01	182
2018-10-02	145
2018-10-03	143
2018-10-04	179
2018-10-05	182
2018-10-06	155
2018-10-07	149

HAMILTON NG911

Menu | Change Chart Type | Select Start | Select End | Calhoun County | Print Page

Each report has the same options to change the chart type, date range select, etc. In this chart you will see calls by the hour and class of service. They are color coded below. If you hover over each one you will see the count for each class of service. The counts are listed below as well. Whether you are running reports that are standardized or from the ESRP, you will have the same options that we have viewed.



Copy CSV PDF

Search:

Average	3.39	2.45	1.94	1.90	2.23	2.35	3.13	4.13	5.90	6.35	5.58	7.06	7.23	7.32	8.03	8.00	7.32	9.45	7.55	7.39	6.77	5.52	4.77	4.39
Totals	105 (2.6%)	76 (1.9%)	60 (1.5%)	59 (1.5%)	69 (1.7%)	73 (1.8%)	97 (2.4%)	128 (3.2%)	183 (4.5%)	197 (4.9%)	173 (4.3%)	219 (5.4%)	224 (5.6%)	227 (5.6%)	249 (6.2%)	248 (6.1%)	227 (5.6%)	293 (7.3%)	234 (5.8%)	229 (5.7%)	210 (5.2%)	171 (4.2%)	148 (3.7%)	136 (3.4%)

CallDate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2018-10-01	6	3	1	3	3	1	4	8	7	5	8	6	3	21	11	14	11	16	6	11	5	2	9	7
2018-10-02	3	3	3	3	1	3	3	7	11	7	7	3	15	7	5	7	13	8	9	7	5	5	5	3
2018-10-03	3	0	2	1	0	0	1	3	5	13	3	3	6	2	4	6	5	5	8	6	10	6	3	5
2018-10-04	5	1	3	3	1	0	3	5	9	6	12	7	5	18	13	14	8	26	15	7	9	5	1	2

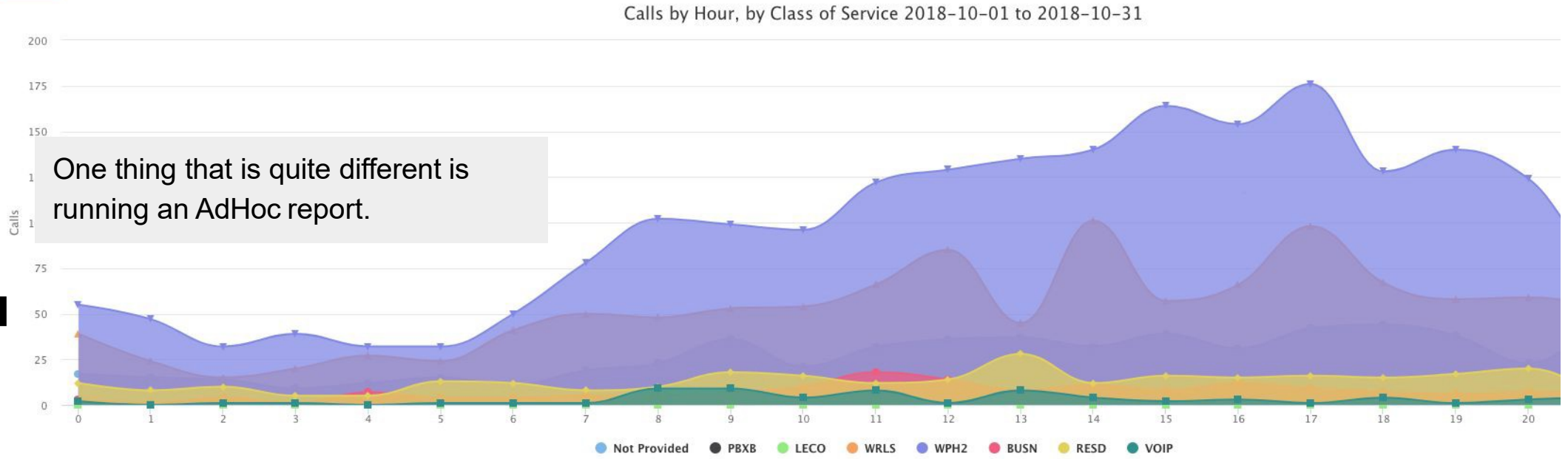
HAMILTON NG911

911 Logix

- Standardized Reports
- Network Reporting
- ESRP Reporting
- AdHoc
- Raw Data
- Information
- Contact
- Switch Theme
- Sign Out, rmartinez

Menu | Change Chart Type | Select Start | Select End | Calhoun County | Print Page

One thing that is quite different is running an AdHoc report.

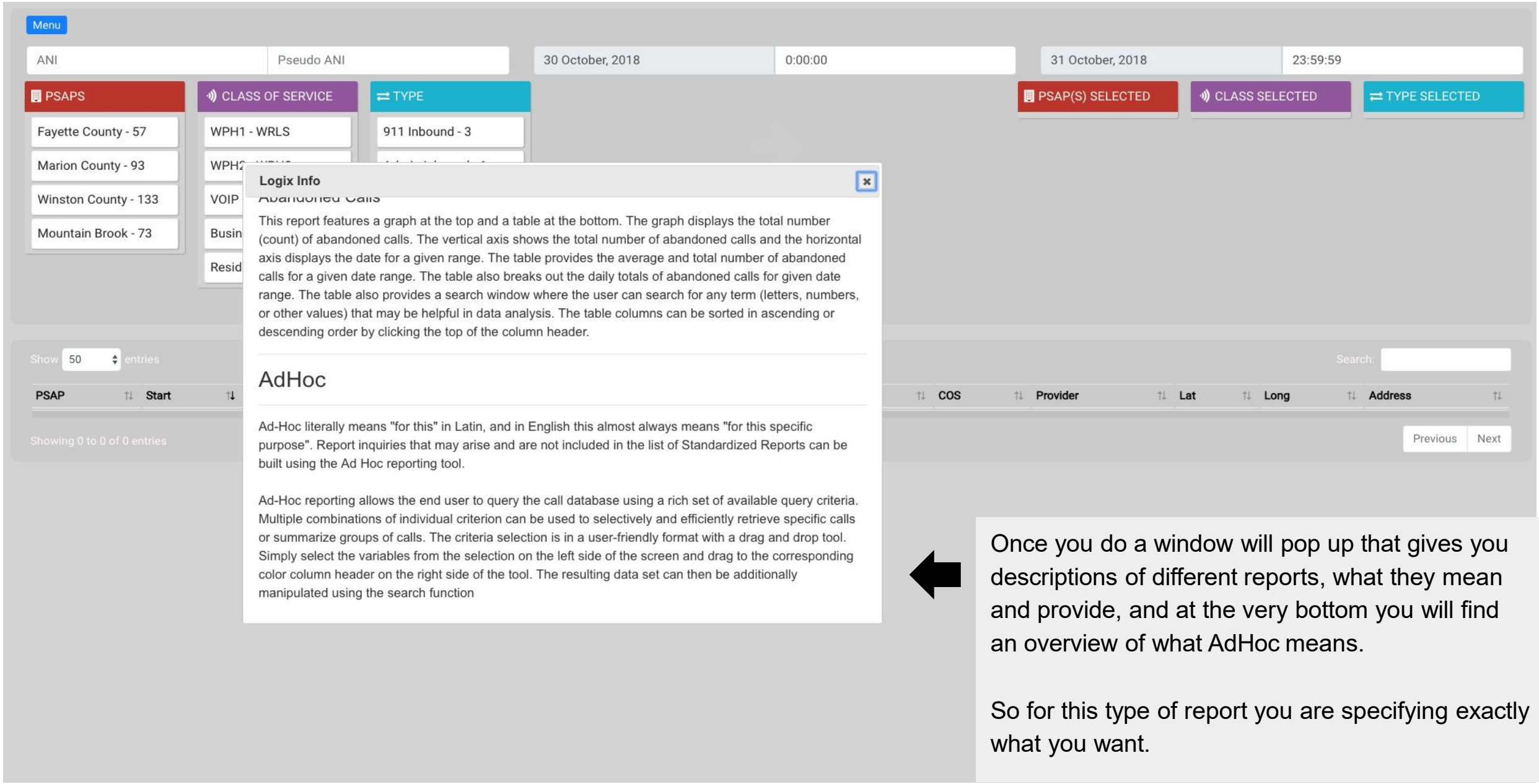


Copy | CSV | PDF

Average	3.39	2.45	1.94	1.90	2.23	2.35	3.13	4.13	5.90	6.35	5.58	7.06	7.23	7.32	8.03	8.00	7.32	9.45	7.55	7.39	6.77
Totals	105 (2.6%)	76 (1.9%)	60 (1.5%)	59 (1.5%)	69 (1.7%)	73 (1.8%)	97 (2.4%)	128 (3.2%)	183 (4.5%)	197 (4.9%)	173 (4.3%)	219 (5.4%)	224 (5.6%)	227 (5.6%)	249 (6.2%)	248 (6.1%)	227 (5.6%)	293 (7.3%)	234 (5.8%)	229 (5.7%)	210 (5.2%)

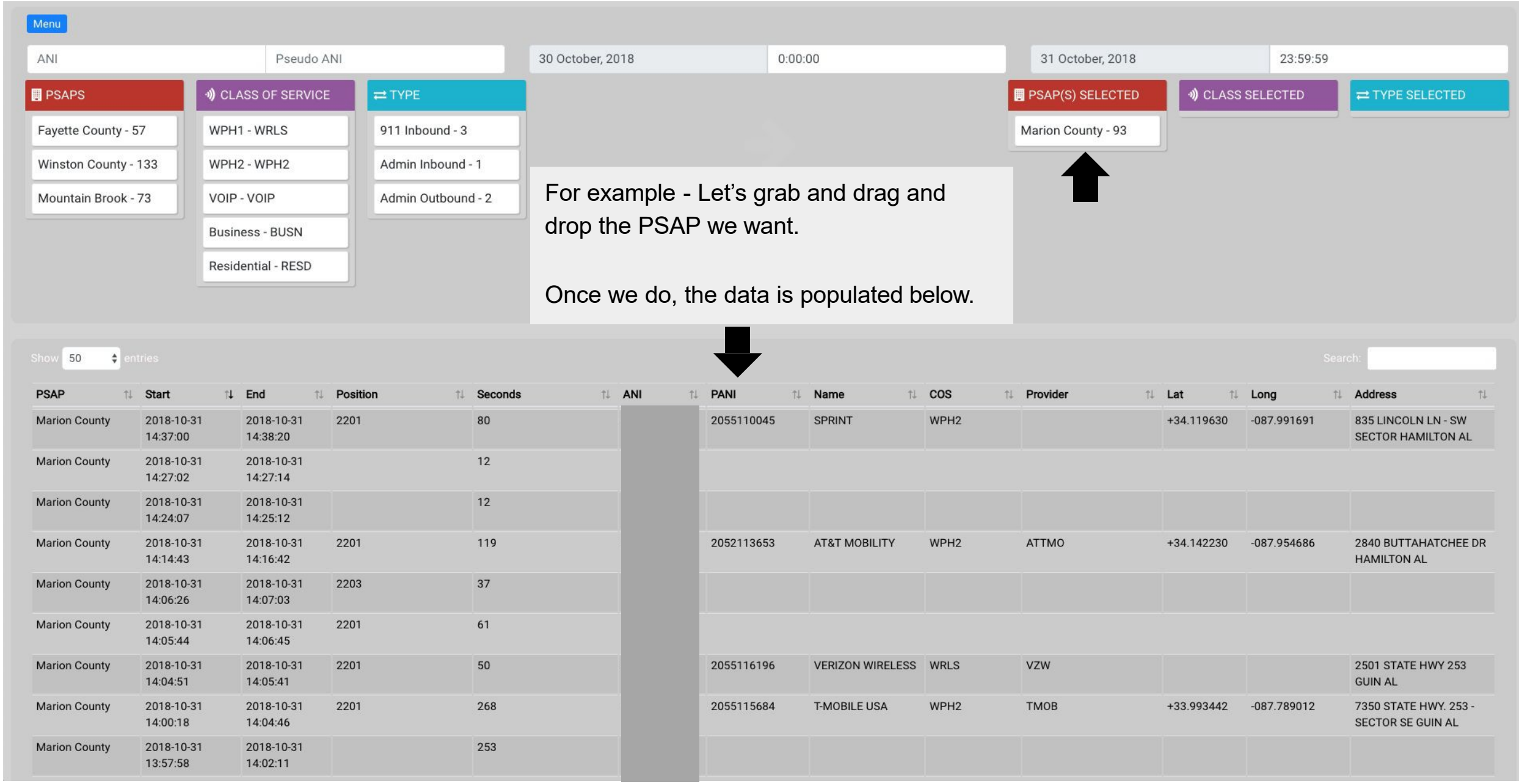
CallDate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2018-10-01	6	3	1	3	3	1	4	8	7	5	8	6	3	21	11	14	11	16	6	11	5
2018-10-02	3	3	3	3	1	3	3	7	11	7	7	3	15	7	5	7	13	8	9	7	5
2018-10-03	3	0	2	1	0	0	1	3	5	13	3	3	6	2	4	6	5	5	8	6	10
2018-10-04	5	1	3	3	1	0	3	5	9	6	12	7	5	18	13	14	8	26	15	7	9

HAMILTON NG911

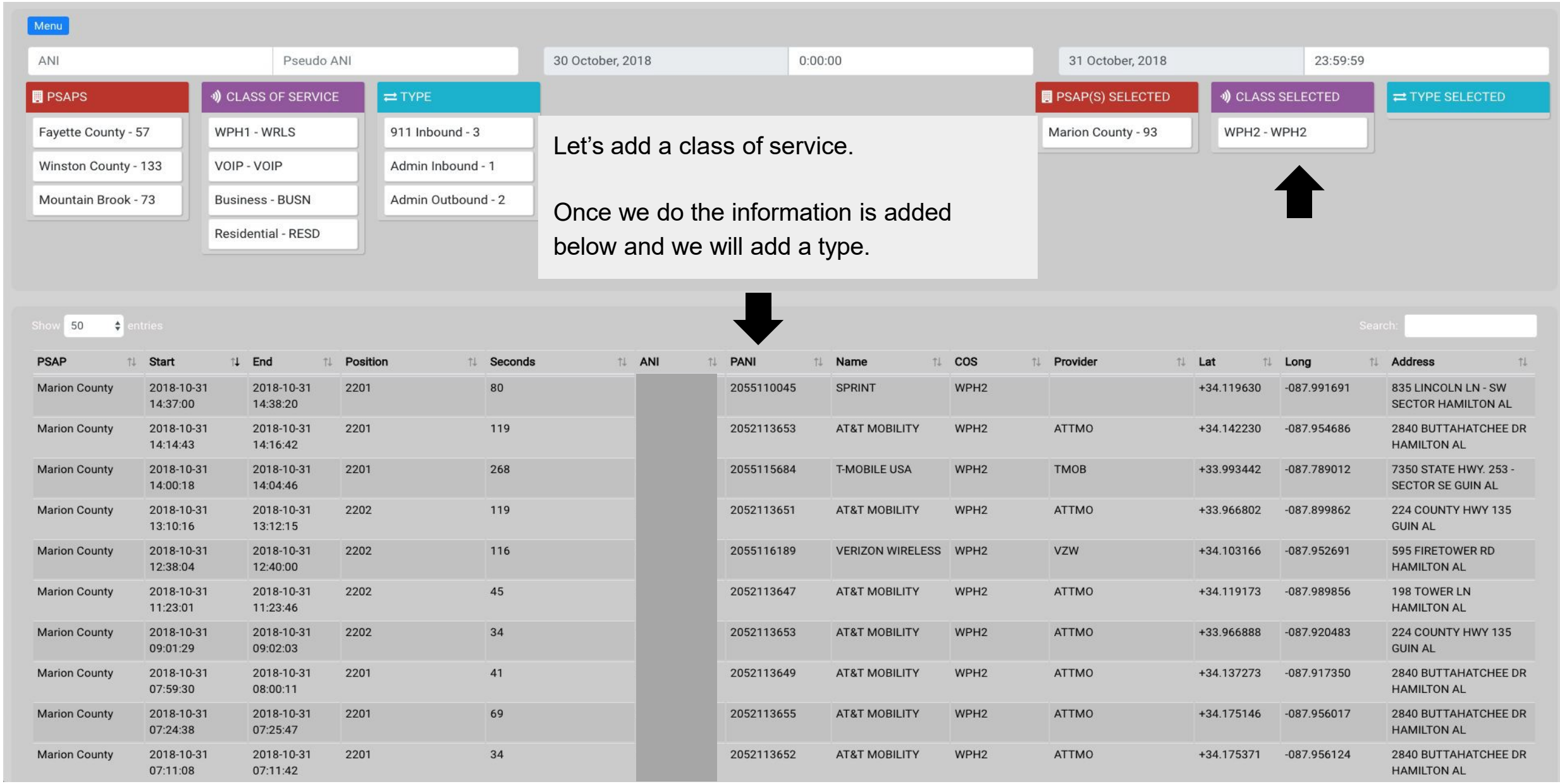


Once you do a window will pop up that gives you descriptions of different reports, what they mean and provide, and at the very bottom you will find an overview of what AdHoc means.

So for this type of report you are specifying exactly what you want.



PSAP	Start	End	Position	Seconds	ANI	PANI	Name	COS	Provider	Lat	Long	Address
Marion County	2018-10-31 14:37:00	2018-10-31 14:38:20	2201	80		2055110045	SPRINT	WPH2		+34.119630	-087.991691	835 LINCOLN LN - SW SECTOR HAMILTON AL
Marion County	2018-10-31 14:27:02	2018-10-31 14:27:14		12								
Marion County	2018-10-31 14:24:07	2018-10-31 14:25:12		12								
Marion County	2018-10-31 14:14:43	2018-10-31 14:16:42	2201	119		2052113653	AT&T MOBILITY	WPH2	ATTMO	+34.142230	-087.954686	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 14:06:26	2018-10-31 14:07:03	2203	37								
Marion County	2018-10-31 14:05:44	2018-10-31 14:06:45	2201	61								
Marion County	2018-10-31 14:04:51	2018-10-31 14:05:41	2201	50		2055116196	VERIZON WIRELESS	WRLS	VZW			2501 STATE HWY 253 GUIN AL
Marion County	2018-10-31 14:00:18	2018-10-31 14:04:46	2201	268		2055115684	T-MOBILE USA	WPH2	TMOB	+33.993442	-087.789012	7350 STATE HWY. 253 - SECTOR SE GUIN AL
Marion County	2018-10-31 13:57:58	2018-10-31 14:02:11		253								



PSAP	Start	End	Position	Seconds	ANI	PANI	Name	COS	Provider	Lat	Long	Address
Marion County	2018-10-31 14:37:00	2018-10-31 14:38:20	2201	80		2055110045	SPRINT	WPH2		+34.119630	-087.991691	835 LINCOLN LN - SW SECTOR HAMILTON AL
Marion County	2018-10-31 14:14:43	2018-10-31 14:16:42	2201	119		2052113653	AT&T MOBILITY	WPH2	ATTMO	+34.142230	-087.954686	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 14:00:18	2018-10-31 14:04:46	2201	268		2055115684	T-MOBILE USA	WPH2	TMOB	+33.993442	-087.789012	7350 STATE HWY. 253 - SECTOR SE GUIN AL
Marion County	2018-10-31 13:10:16	2018-10-31 13:12:15	2202	119		2052113651	AT&T MOBILITY	WPH2	ATTMO	+33.966802	-087.899862	224 COUNTY HWY 135 GUIN AL
Marion County	2018-10-31 12:38:04	2018-10-31 12:40:00	2202	116		2055116189	VERIZON WIRELESS	WPH2	VZW	+34.103166	-087.952691	595 FIRETOWER RD HAMILTON AL
Marion County	2018-10-31 11:23:01	2018-10-31 11:23:46	2202	45		2052113647	AT&T MOBILITY	WPH2	ATTMO	+34.119173	-087.989856	198 TOWER LN HAMILTON AL
Marion County	2018-10-31 09:01:29	2018-10-31 09:02:03	2202	34		2052113653	AT&T MOBILITY	WPH2	ATTMO	+33.966888	-087.920483	224 COUNTY HWY 135 GUIN AL
Marion County	2018-10-31 07:59:30	2018-10-31 08:00:11	2201	41		2052113649	AT&T MOBILITY	WPH2	ATTMO	+34.137273	-087.917350	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 07:24:38	2018-10-31 07:25:47	2201	69		2052113655	AT&T MOBILITY	WPH2	ATTMO	+34.175146	-087.956017	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 07:11:08	2018-10-31 07:11:42	2201	34		2052113652	AT&T MOBILITY	WPH2	ATTMO	+34.175371	-087.956124	2840 BUTTAHATCHEE DR HAMILTON AL

Menu

ANI | Pseudo ANI | 30 October, 2018 | 0:00:00 | 31 October, 2018 | 23:59:59

PSAPS
- Fayette County - 57
- Winston County - 133
- Mountain Brook - 73

CLASS OF SERVICE
- WPH1 - WRLS
- VOIP - VOIP
- Business - BUSN
- Residential - RESD

TYPE
- Admin Inbound - 1
- Admin Outbound - 2

PSAP(S) SELECTED
- Marion County - 93

CLASS SELECTED
- WPH2 - WPH2

TYPE SELECTED
- 911 Inbound - 3

We will add a type. Now we have this specific report to scroll through.

Show 50 entries

Search:

PSAP	Start	End	Position	Seconds	ANI	PANI	Name	COS	Provider	Lat	Long	Address
Marion County	2018-10-31 14:37:00	2018-10-31 14:38:20	2201	80		2055110045	SPRINT	WPH2		+34.119630	-087.991691	835 LINCOLN LN - SW SECTOR HAMILTON AL
Marion County	2018-10-31 14:14:43	2018-10-31 14:16:42	2201	119		2052113653	AT&T MOBILITY	WPH2	ATTMO	+34.142230	-087.954686	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 14:00:18	2018-10-31 14:04:46	2201	268		2055115684	T-MOBILE USA	WPH2	TMOB	+33.993442	-087.789012	7350 STATE HWY. 253 - SECTOR SE GUIN AL
Marion County	2018-10-31 13:10:16	2018-10-31 13:12:15	2202	119		2052113651	AT&T MOBILITY	WPH2	ATTMO	+33.966802	-087.899862	224 COUNTY HWY 135 GUIN AL
Marion County	2018-10-31 12:38:04	2018-10-31 12:40:00	2202	116		2055116189	VERIZON WIRELESS	WPH2	VZW	+34.103166	-087.952691	595 FIRETOWER RD HAMILTON AL
Marion County	2018-10-31 11:23:01	2018-10-31 11:23:46	2202	45		2052113647	AT&T MOBILITY	WPH2	ATTMO	+34.119173	-087.989856	198 TOWER LN HAMILTON AL
Marion County	2018-10-31 09:01:29	2018-10-31 09:02:03	2202	34		2052113653	AT&T MOBILITY	WPH2	ATTMO	+33.966888	-087.920483	224 COUNTY HWY 135 GUIN AL
Marion County	2018-10-31 07:59:30	2018-10-31 08:00:11	2201	41		2052113649	AT&T MOBILITY	WPH2	ATTMO	+34.137273	-087.917350	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 07:24:38	2018-10-31 07:25:47	2201	69		2052113655	AT&T MOBILITY	WPH2	ATTMO	+34.175146	-087.956017	2840 BUTTAHATCHEE DR HAMILTON AL
Marion County	2018-10-31 07:11:08	2018-10-31 07:11:42	2201	34		2052113652	AT&T MOBILITY	WPH2	ATTMO	+34.175371	-087.956124	2840 BUTTAHATCHEE DR HAMILTON AL

HAMILTON NG911

911 Logix

- Standardized Reports
- Network Reporting
- ESRP Reporting
- AdHoc
- Raw Data
- Information
- Contact
- Switch Theme
- Sign Out, rmartinez

Menu

ANI | Pseudo ANI | 30 October, 2018 | 0:00:00 | 31 October, 2018 | 23:59:5

PSAPS	CLASS OF SERVICE	TYPE	PSAP(S) SELECTED	CLASS SELECTED
Fayette County - 57	WPH1 - WRLS		Marion County - 93	WPH2 - WPH2
Winston County - 133	VOIP - VOIP			
Mountain Brook - 73	Business - BUSN			
	Residential - RESD			

The raw data is just that. You can press the tab and simply see the raw data that is being logged for each call that comes into your PSAP.

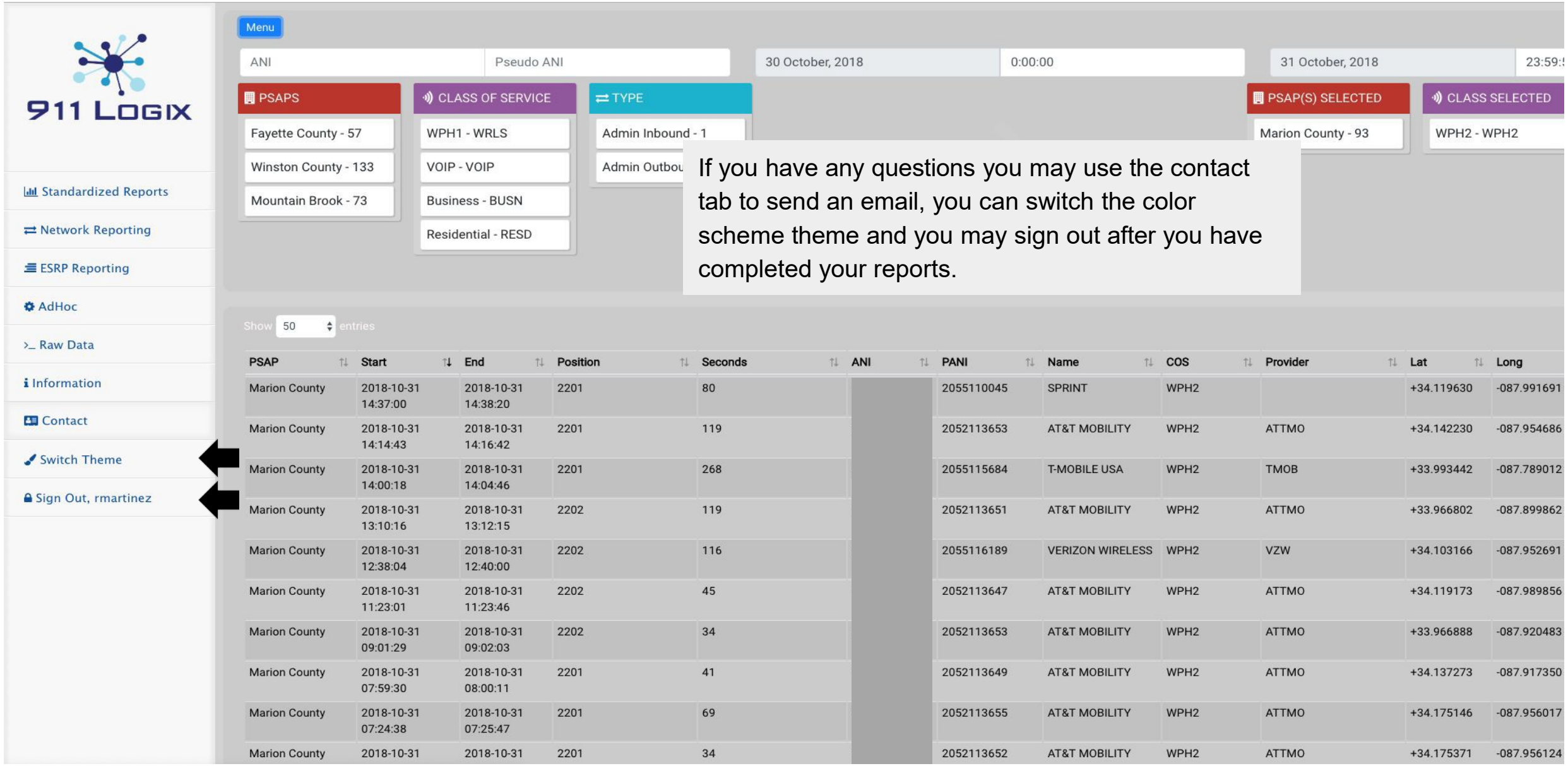
Show 50 entries

PSAP	Start	End	Position
Marion County	2018-10-31 14:37:00	2018-10-31 14:38:20	2201
Marion County	2018-10-31 14:14:43	2018-10-31 14:16:42	2201
Marion County	2018-10-31 14:00:18	2018-10-31 14:04:46	2201
Marion County	2018-10-31 13:10:16	2018-10-31 13:12:15	2202
Marion County	2018-10-31 12:38:04	2018-10-31 12:40:00	2202
Marion County	2018-10-31 11:23:01	2018-10-31 11:23:46	2202
Marion County	2018-10-31 09:01:29	2018-10-31 09:02:03	2202
Marion County	2018-10-31 07:59:30	2018-10-31 08:00:11	2201
Marion County	2018-10-31 07:24:38	2018-10-31 07:25:47	2201
Marion County	2018-10-31	2018-10-31	2201

Menu | All PSAPs

21:11:51.879Z Dothan - UNC 00000 Z
21:11:51.879Z Dothan - X-085.363212 Y+031.285383 CF0
21:11:51.879Z Dothan - P#334-723-2430 ALT#334-322-9780
21:11:51.879Z Dothan - ESN 352
21:11:51.879Z Dothan - SW SECTOR
21:11:51.879Z Dothan - Dothan AL
21:11:51.879Z Dothan - LEC Veriz
21:11:51.879Z Dothan - Grey Hodges RD
21:11:51.879Z Dothan - 331 E
21:11:51.879Z Dothan - VERIZON WIRELESS
21:11:51.879Z Dothan - SEIZE 2018-11-08 15:11:29|TRUNK 52|CLASS WPH1|ANI 3343229780|RING 2018-11-08 15:11:29|ANSWER 2018-11-08 15:11:29|POSITION 3|HANGUP null|RELEASE null|ABANDONED false|TRANSFER null|DESTINATION null|ALI 334-723-2430 16:11:27 11082018
21:11:51.878Z Dothan - UNC 00000 Z
21:11:51.878Z Dothan - X-085.363212 Y+031.285383 CF0
21:11:51.878Z Dothan - P#334-723-2430 ALT#334-322-9780
21:11:51.878Z Dothan - ESN 352
21:11:51.878Z Dothan - SW SECTOR
21:11:51.878Z Dothan - Dothan AL
21:11:51.877Z Dothan - LEC Veriz
21:11:51.877Z Dothan - Grey H
21:11:51.877Z Dothan - 331 E WPH1
21:11:51.877Z Dothan - VERIZON WIRELESS
21:11:51.877Z Dothan - SEIZE 2018-11-08 15:11:29|TRUNK 52|CLASS WPH1|ANI 3343229780|RING 2018-11-08 15:11:29|ANSWER 2018-11-08 15:11:29|POSITION 3|HANGUP 2018-11-08 15:11:49|RELEASE 2018-11-08 15:11:49|ABANDONED false|TRANSFER null|DESTINATION null|ALI 334-723-2430 16:11:27 11082018
21:11:46.993Z Calhoun County - /nAgent In ACD Nov/08/18 15:11:42 CST Device Name POS7 Reason Manual ready .....
21:11:34.737Z Mountain Brook 911 - --- --- --- --- --- --- --- --- --- --- --- --- ---
21:11:31.677Z Mountain Brook 911 - ANI 2145519569 Call 2468020 Is Selected By 2202 Nov/08/18 15:10:10 CST Call 2468020 Cellular Call Nov/08/18 15:10:10 CST Call 2468020 CPN: 2145519569

HAMILTON NG911



HAMILTON NG911

Questions?

Hamilton NG911
www.HamiltonNG911.com
NG911@hamiltontel.com
800.821.1831

HAMILTON NG911

HAMILTON APPENDIX 16: HAMILTON CERTIFICATE OF PUBLIC NECESSITY

BEFORE THE NEBRASKA PUBLIC SERVICE COMMISSION

In the Matter of the Application of Hamilton NG911, Inc., Aurora, Nebraska, seeking authority to provide competitive local exchange telecommunications services within the State of Nebraska.	))))))	Application No. C-5109 GRANTED Entered: June 2, 2020

BY THE COMMISSION:

On April 2, 2020 an application was filed by Hamilton NG911, Inc. ("Hamilton" or "Applicant") of Aurora, Nebraska, seeking authority to provide competitive local exchange telecommunications services within the State of Nebraska. Notice of the application was published in The Daily Record, Omaha, Nebraska, on April 8, 2020. No protests were filed; therefore, this application is processed pursuant to the Commission's Rules of Modified Procedure.

Applicant is a Nebraska corporation authorized to do business in the State of Nebraska. Applicant has been authorized by the Secretary of State to operate in Nebraska. Applicant does not have any pending applications for certification to provide telecommunications services in any other state. Applicant currently only operates within Nebraska. No officer, director, or shareholder having 5% or more of Applicant' s voting securities nor any of Applicant' s business operations has been involved in a formal complaint or other investigatory or enforcement proceeding.

Applicant requests authority to provide local exchange telecommunications services throughout the State of Nebraska. Applicant plans to provide a portfolio of Next Gen 9-1-1 services including Internet Protocol (IP) based 9-1-1 call routing, database services and management, and network services designed to make it easier to move from the current legacy 9-1-1 system to a Next Gen 9-1-1 system. Applicant does not intend to offer local dial tone services to businesses or residences, but will comply with the requirements for directory assistance, operator assistance, and for Telecommunications Relay Service if local dial tone services are offered in the future.

Applicant states it possesses the requisite financial, technical, and managerial expertise to provide the proposed services. Applicant will draw on the management resources of its

affiliates and certain consultants for planning, marketing, network service development, provisioning and delivery, and legal and regulatory assistance. Applicant is a wholly owned subsidiary of Nedelco, Inc., which is a holding company for the applicant and its affiliates. Applicant intends to rely on the financial resources of its parent company. Applicant is not a public company and does not publish annual reports. In Exhibit 4, Applicant provided a true and correct copy of its financial statements for the period ending in December 31, 2019. Nedelco, Inc. has provided startup funding to Applicant and will maintain the minimum positive capitalization as required by the Commission.

Applicant states that a grant of the application is in the public interest because the public will benefit from greater consumer choice through the broadening of telecommunications service alternatives and affordable rates maintained by competition. Further, Applicant states its provision of competitive local exchange service will preserve and advance universal service, protect the public safety and welfare, ensure the continuous quality of telecommunications services, and safeguard the rights of consumers.

O P I N I O N A N D F I N D I N G S

The Commission considers this application for authority in light of the following criteria and standards established in the Commission's telecommunications rules:

(a) Whether the Applicant has provided the information required by the Commission;
(b) Whether the Applicant has provided a performance bond, if required;
(c) Whether the Applicant possesses adequate financial resources to provide the proposed service;
(d) Whether the Applicant possesses adequate technical competence and resources to provide the proposed service;
(e) Whether the Applicant possesses the adequate managerial competence to provide the proposed service; and
(f) Whether granting the Applicant a certificate preserves and advances universal service, protects the public safety and welfare, ensures the continued quality of telecommunications services and safeguards the rights of consumers, pursuant to Section 253(b) of the Act.

Applicant has demonstrated that it meets the standards of financial, technical, and managerial competence and all other criteria necessary to provide local exchange services in the State of Nebraska.

These opinions and findings carry no precedential value other than establishing minimum standards and criteria to apply when considering applications to provide local exchange services. All telecommunications carriers seeking such a certificate must demonstrate that they meet, at a minimum, the standards and criteria set forth herein.

Before the Applicant is allowed to provide local exchange service to its users, it must either:

1. Through negotiation or arbitration, reach an interconnection/resale agreement with the pertinent incumbent local exchange carrier and receive Commission approval of the interconnection/resale agreement; or
2. In the event a certified local exchange carrier provides a wholesale tariff, purchase rates from that tariff, file its own tariff and receive Commission approval of its tariff.

This order does not terminate, waive or in any manner diminish the exemptions and protections created by the Act for rural carriers, as defined by the Act. This order does not address the issue of rural local exchange carrier exemption under the Act. Rural exemptions may be terminated, suspended or modified only as provided in section 251(f) of the Act.

Prior to providing service in any area in the State of Nebraska, Applicant must file tariffs in accordance with the provisions of Section 002.21 of the Neb. Admin. R. & Regs. Title 291, Ch. 5. 2

Upon the offering of local exchange services in the State of Nebraska, Applicant would be subject to the same laws, rules and regulations, both federal and state (including any laws, rules or regulations regarding universal service, restrictions on joint marketing and quality of service), applicable to any other exchange company except those obligations imposed on ILECs pursuant to Section 251(c) of the Act.

O R D E R

IT IS THEREFORE ORDERED by the Nebraska Public Service Commission that Application C-5109 be, and is hereby, granted.

IT IS FURTHER ORDERED that Applicant is obligated to abide by the same laws, rules and regulations, both federal and state (including any laws, rules or regulations regarding universal service, restrictions on joint marketing and quality of service), applicable to any other local exchange carriers, except obligations imposed on incumbent local exchange carriers pursuant to Section 251(c) of the Act.

IT IS FURTHER ORDERED that, to the extent Applicant provides access line service as referenced in the Telecommunications Relay System Act, Neb. Rev. Stat. §§ 86-301 through 86-315(Relay Act) and defined in Neb. Admin. R. & Regs. Title 291, Ch. 5 § 001.01B, the Applicant shall collect from its subscribers a surcharge (Relay Surcharge) pursuant to the relay act and the Commission's annual orders establishing the amount of the surcharge, and shall remit to the Commission the proceeds from the relay surcharge as provided by the Relay Act.

IT IS FURTHER ORDERED that the Applicant comply with all necessary statutes and Commission Rules and Regulations as they pertain to the Nebraska Universal Service Fund.

IT IS FURTHER ORDERED that Applicant shall file, in accordance with the applicable statutes, on or before April 30 of each year, an annual report with the Commission consisting of: (a) a copy of any report filed with the Federal Communications Commission; (b) a copy of any annual report to stockholders; and (c) a copy of the latest form 10-K filed with the Securities Exchange Commission. If such reports are unavailable, Applicant shall file a balance sheet and income statement for the previous year of operation, and for the State of Nebraska on a combined interstate-intrastate basis, the investment in the telephone plant and equipment located within the state, accumulated depreciation thereon, operating revenues, operating expenses and taxes.

IT IS FURTHER ORDERED that within 30 days from the entry of this order that the Applicant file a tariff and pay appropriate filing fees with the Commission as required by state statutes and the Commission's regulations.

IT IS FURTHER ORDERED that this order be, and is hereby, made the Commission's official certificate of Public Convenience and

Necessity to the Applicant to provide local exchange telecommunications services in the State of Nebraska.

ENTERED AND MADE EFFECTIVE at Lincoln, Nebraska, this 2nd day of June, 2020.

NEBRASKA PUBLIC SERVICE COMMISSION

COMMISSIONERS CONCURRING:

Chair

ATTEST:

Executive Director

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 C ESInet and 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.
- If more rows are needed in each region, you can insert additional rows.
- 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 Svc 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 ESInet, **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.

ESInet Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services IP Network services (hardware, software, connectivity, training, maintenance, etc.) for each region. Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly per person amounts in cents**. The monthly amounts are automatically multiplied by the population of the region and by 12 months.

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.

ESInet Milestones	
Milestone 1: **Region 1** regional host connection and testing acceptance	25920.08
Milestone 2: **Region 2** regional host connection and testing acceptance	25920.08
Milestone 3: **Region 3** regional host connection and testing acceptance	25920.08
Milestone 4: **Region 4** regional host connection and testing acceptance	25920.08
Milestone 5: **Region 5** regional host connection and testing acceptance	25920.08
Milestone 6: **Region 6** regional host connection and testing acceptance	25919.94
Milestone 7: **Region 7** regional host connection and testing acceptance	25920.08
TOTAL	181440.42

NGCS Milestones	
Milestone 1: **Region 1** deployments complete	298,145.23
Milestone 2: **Region 2** deployments complete	508,323.66
Milestone 3: **Region 3** deployments complete	724,266.27
Milestone 4: **Region 4** deployments complete	106,236.51
Milestone 5: **Region 5** deployments complete	232,701.04
Milestone 6: **Region 6** deployments complete	177,676.71
Milestone 7: **Region 7** deployments complete	135,213.60
TOTAL	2182563.02

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name	Hamilton NG911, Inc.														
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]**
ESInet	181,440.42	142,260.67	0.00	142,260.67	0.00	142,260.67	0.00	142,260.67	0.00	142,260.67	181,035.12	181,035.12	181,035.12	181,035.12	181,035.12
LNG	106,427.06	289,390.20	0.00	289,390.20	0.00	289,390.20	0.00	289,390.20	0.00	289,390.20	317,171.66	317,171.66	317,171.66	317,171.66	317,171.66
BCF	374,165.86	312,541.42	0.00	312,541.42	0.00	312,541.42	0.00	312,541.42	0.00	312,541.42	395,885.79	395,885.79	395,885.79	395,885.79	395,885.79
ESRP & PRF	1,122,497.57	770,935.49	0.00	770,935.49	0.00	770,935.49	0.00	770,935.49	0.00	770,935.49	1,016,338.38	1,016,338.38	1,016,338.38	1,016,338.38	1,016,338.38
ECRF & LVF	271,061.56	229,197.04	0.00	229,197.04	0.00	229,197.04	0.00	229,197.04	0.00	229,197.04	287,075.08	287,075.08	287,075.08	287,075.08	287,075.08
SI	67,765.39	57,878.04	0.00	57,878.04	0.00	57,878.04	0.00	57,878.04	0.00	57,878.04	71,768.77	71,768.77	71,768.77	71,768.77	71,768.77
LDB	240,645.58	150,482.90	0.00	150,482.90	0.00	150,482.90	0.00	150,482.90	0.00	150,482.90	203,730.70	203,730.70	203,730.70	203,730.70	203,730.70
MISC	0.00	259,293.62	0.00	259,293.62	0.00	259,293.62	0.00	259,293.62	0.00	259,293.62	266,238.98	266,238.98	266,238.98	266,238.98	266,238.98
Total	2,364,003.44	2,211,979.38	0.00	2,211,979.38	0.00	2,211,979.38	0.00	2,211,979.38	0.00	2,211,979.38	2,739,244.49	2,739,244.49	2,739,244.49	2,739,244.49	2,739,244.49

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)	4,575,982.82	2,211,979.38	2,211,979.38	2,211,979.38	2,211,979.38	2,739,244.49	2,739,244.49	2,739,244.49	2,739,244.49	2,739,244.49
Initial Contract (5 Year NRC+MRC)	13,423,900.35									
+ Optional Year 6 (6 Year NRC+MRC)	16,163,144.84									
+ Optional Years 7 (7 Year NRC+MRC)	18,902,389.33									
+ Optional Years 8 (8 Year NRC+MRC)	21,641,633.82									
+ Optional Years 9 (9 Year NRC+MRC)	24,380,878.31									
+ Optional Years 10 (10 Year NRC+MRC)	27,120,122.80									

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	1,929,268

Bidder Name:	0
Date (MM/DD/YYYY):	1/0/1900

Emergency Services IP Network	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															
200 Mbps Primary Circuit w/ Edge Hardware - Buffalo Host	12,960.0400	0.0021		0.0021		0.0021		0.0021		0.0021	0.0030	0.0030	0.0030	0.0030	0.0030
200 Mbps Primary Circuit w/ Edge Hardware - Dawson Host	12,960.0400	0.0021		0.0021		0.0021		0.0021		0.0021	0.0030	0.0030	0.0030	0.0030	0.0030
Back-up Internet w/ VPN - Buffalo Host		0.0006		0.0006		0.0006		0.0006		0.0006	0.0006	0.0006	0.0006	0.0006	0.0006
Back-up Internet w/ VPN - Dawson Host		0.0006		0.0006		0.0006		0.0006		0.0006	0.0006	0.0006	0.0006	0.0006	0.0006
Bidder Input															
Bidder Input															
NRC/MRC REGION 1 TOTAL	25,920.0800	16,795.0584	0.0000	16,795.0584	0.0000	16,795.0584	0.0000	16,795.0584	0.0000	16,795.0584	22,393.4112	22,393.4112	22,393.4112	22,393.4112	22,393.4112
Region Two Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68508 Host	12,960.0400	0.0011		0.0011		0.0011		0.0011		0.0011	0.0015	0.0015	0.0015	0.0015	0.0015
200 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68512 Host	12,960.0400	0.0011		0.0011		0.0011		0.0011		0.0011	0.0015	0.0015	0.0015	0.0015	0.0015
Back-up Internet w/ VPN - Lincoln 68508 Host		0.0003		0.0003		0.0003		0.0003		0.0003	0.0003	0.0003	0.0003	0.0003	0.0003
Back-up Internet w/ VPN - Lincoln 68512 Host		0.0003		0.0003		0.0003		0.0003		0.0003	0.0003	0.0003	0.0003	0.0003	0.0003
Bidder Input															
Bidder Input															
NRC/MRC REGION 2 TOTAL	25,920.0800	17,207.4336	0.0000	17,207.4336	0.0000	17,207.4336	0.0000	17,207.4336	0.0000	17,207.4336	22,123.8432	22,123.8432	22,123.8432	22,123.8432	22,123.8432
Region Three Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Douglas Host	12,960.0400	0.0013		0.0013		0.0013		0.0013		0.0013	0.0016	0.0016	0.0016	0.0016	0.0016
200 Mbps Primary Circuit w/ Edge Hardware - Pottawatomie Host	12,960.0400	0.0007		0.0007		0.0007		0.0007		0.0007	0.0010	0.0010	0.0010	0.0010	0.0010
Back-up Internet w/ VPN - Douglas Host		0.0002		0.0002		0.0002		0.0002		0.0002	0.0002	0.0002	0.0002	0.0002	0.0002
Back-up Internet w/ VPN - Pottawatomie Host		0.0002		0.0002		0.0002		0.0002		0.0002	0.0002	0.0002	0.0002	0.0002	0.0002
Bidder Input															
Bidder Input															
NRC/MRC REGION 3 TOTAL	25,920.0800	22,233.7728	0.0000	22,233.7728	0.0000	22,233.7728	0.0000	22,233.7728	0.0000	22,233.7728	27,792.2160	27,792.2160	27,792.2160	27,792.2160	27,792.2160
Region Four Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Boyd Host	12,960.0400	0.0195		0.0195		0.0195		0.0195		0.0195	0.0277	0.0277	0.0277	0.0277	0.0277
200 Mbps Primary Circuit w/ Edge Hardware - Cherry Host	12,960.0400	0.0195		0.0195		0.0195		0.0195		0.0195	0.0277	0.0277	0.0277	0.0277	0.0277
Back-up Internet w/ VPN - Boyd Host		0.0055		0.0055		0.0055		0.0055		0.0055	0.0056	0.0056	0.0056	0.0056	0.0056
Back-up Internet w/ VPN - Cherry Host		0.0055		0.0055		0.0055		0.0055		0.0055	0.0056	0.0056	0.0056	0.0056	0.0056
Bidder Input															
Bidder Input															
NRC/MRC REGION 4 TOTAL	25,920.0800	16,936.2000	0.0000	16,936.2000	0.0000	16,936.2000	0.0000	16,936.2000	0.0000	16,936.2000	22,559.0184	22,559.0184	22,559.0184	22,559.0184	22,559.0184
Region Five Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Columbus Host	12,960.0400	0.0045		0.0045		0.0045		0.0045		0.0045	0.0058	0.0058	0.0058	0.0058	0.0058
200 Mbps Primary Circuit w/ Edge Hardware - Saunders Host	12,960.0400	0.0063		0.0063		0.0063		0.0063		0.0063	0.0076	0.0076	0.0076	0.0076	0.0076
Back-up Internet w/ VPN - Columbus Host		0.0009		0.0009		0.0009		0.0009		0.0009	0.0009	0.0009	0.0009	0.0009	0.0009
Back-up Internet w/ VPN - Saunders Host		0.0009		0.0009		0.0009		0.0009		0.0009	0.0009	0.0009	0.0009	0.0009	0.0009
Bidder Input															
Bidder Input															
NRC/MRC REGION 5 TOTAL	25,920.0800	27,279.9576	0.0000	27,279.9576	0.0000	27,279.9576	0.0000	27,279.9576	0.0000	27,279.9576	32,909.1552	32,909.1552	32,909.1552	32,909.1552	32,909.1552
Region Six Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Norfolk	12,960.0400	0.0045		0.0045		0.0045		0.0045		0.0045	0.0065	0.0065	0.0065	0.0065	0.0065
200 Mbps Primary Circuit w/ Edge Hardware - South Sioux City	12,959.9000	0.0063		0.0063		0.0063		0.0063		0.0063	0.0084	0.0084	0.0084	0.0084	0.0084
Back-up Internet w/ VPN - Norfolk		0.0014		0.0014		0.0014		0.0014		0.0014	0.0014	0.0014	0.0014	0.0014	0.0014
Back-up Internet w/ VPN - South Sioux City		0.0014		0.0014		0.0014		0.0014		0.0014	0.0014	0.0014	0.0014	0.0014	0.0014
Bidder Input															
Bidder Input															
NRC/MRC REGION 6 TOTAL	25,919.9400	18,637.9296	0.0000	18,637.9296	0.0000	18,637.9296	0.0000	18,637.9296	0.0000	18,637.9296	24,256.7172	24,256.7172	24,256.7172	24,256.7172	24,256.7172
Region Seven Milestone															
200 Mbps Primary Circuit w/ Edge Hardware - Schuyler Host	12,960.0400	0.0120		0.0120		0.0120		0.0120		0.0120	0.0157	0.0157	0.0157	0.0157	0.0157
200 Mbps Primary Circuit w/ Edge Hardware - Fremont Host	12,960.0400	0.0138		0.0138		0.0138		0.0138		0.0138	0.0176	0.0176	0.0176	0.0176	0.0176
Back-up Internet w/ VPN - Schuyler Host		0.0024		0.0024		0.0024		0.0024		0.0024	0.0025	0.0025	0.0025	0.0025	0.0025
Back-up Internet w/ VPN - Fremont Host		0.0024		0.0024		0.0024		0.0024		0.0024	0.0025	0.0025	0.0025	0.0025	0.0025
Bidder Input															
Bidder Input															
NRC/MRC REGION 7 TOTAL	25,920.0800	23,170.3200	0.0000	23,170.3200	0.0000	23,170.3200	0.0000	23,170.3200	0.0000	23,170.3200	29,000.7600	29,000.7600	29,000.7600	29,000.7600	29,000.7600
ESInet Total	181,440.4200	142,260.6720	0.0000	142,260.6720	0.0000	142,260.6720	0.0000	142,260.6720	0.0000	142,260.6720	181,035.1212	181,035.1212	181,035.1212	181,035.1212	181,035.1212

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Hamilton NG911, Inc.
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															
LNG	14,297.6900	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	14,297.6900	38,877.4500	0.0000	38,877.4500	0.0000	38,877.4500	0.0000	38,877.4500	0.0000	38,877.4500	42,609.6852	42,609.6852	42,609.6852	42,609.6852	42,609.6852
Region Two Milestone															
LNG	28,251.1600	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	28,251.1600	76,818.9000	0.0000	76,818.9000	0.0000	76,818.9000	0.0000	76,818.9000	0.0000	76,818.9000	84,193.5144	84,193.5144	84,193.5144	84,193.5144	84,193.5144
Region Three Milestone															
LNG	42,587.3100	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	42,587.3100	115,800.9000	0.0000	115,800.9000	0.0000	115,800.9000	0.0000	115,800.9000	0.0000	115,800.9000	126,917.7864	126,917.7864	126,917.7864	126,917.7864	126,917.7864
Region Four Milestone															
LNG	1,557.1300	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	1,557.1300	4,234.0500	0.0000	4,234.0500	0.0000	4,234.0500	0.0000	4,234.0500	0.0000	4,234.0500	4,640.5188	4,640.5188	4,640.5188	4,640.5188	4,640.5188
Region Five Milestone															
LNG	9,952.9400	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	9,952.9400	27,063.4500	0.0000	27,063.4500	0.0000	27,063.4500	0.0000	27,063.4500	0.0000	27,063.4500	29,661.5412	29,661.5412	29,661.5412	29,661.5412	29,661.5412
Region Six Milestone															
LNG	6,299.9500	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	6,299.9500	17,130.4500	0.0000	17,130.4500	0.0000	17,130.4500	0.0000	17,130.4500	0.0000	17,130.4500	18,774.9732	18,774.9732	18,774.9732	18,774.9732	18,774.9732
Region Seven Milestone															
LNG	3,480.8800	0.0125		0.0125		0.0125		0.0125		0.0125	0.0137	0.0137	0.0137	0.0137	0.0137
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	3,480.8800	9,465.0000	0.0000	9,465.0000	0.0000	9,465.0000	0.0000	9,465.0000	0.0000	9,465.0000	10,373.6400	10,373.6400	10,373.6400	10,373.6400	10,373.6400
LNG Total	**106,427.0600**	**289,390.2000**	**0.0000**	**289,390.2000**	**0.0000**	**289,390.2000**	**0.0000**	**289,390.2000**	**0.0000**	**289,390.2000**	**317,171.6592**	**317,171.6592**	**317,171.6592**	**317,171.6592**	**317,171.6592**

Bidder Name:	Hamilton NG911, Inc.														
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	50,266.4400	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	50,266.4400	41,987.6460	0.0000	41,987.6460	0.0000	41,987.6460	0.0000	41,987.6460	0.0000	41,987.6460	53,184.3516	53,184.3516	53,184.3516	53,184.3516	53,184.3516
Region Two Milestone															
BCF	99,322.6800	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	99,322.6800	82,964.4120	0.0000	82,964.4120	0.0000	82,964.4120	0.0000	82,964.4120	0.0000	82,964.4120	105,088.2552	105,088.2552	105,088.2552	105,088.2552	105,088.2552
Region Three Milestone															
BCF	149,724.2900	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	149,724.2900	125,064.9720	0.0000	125,064.9720	0.0000	125,064.9720	0.0000	125,064.9720	0.0000	125,064.9720	158,415.6312	158,415.6312	158,415.6312	158,415.6312	158,415.6312
Region Four Milestone															
BCF	5,474.4000	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	5,474.4000	4,572.7740	0.0000	4,572.7740	0.0000	4,572.7740	0.0000	4,572.7740	0.0000	4,572.7740	5,792.1804	5,792.1804	5,792.1804	5,792.1804	5,792.1804
Region Five Milestone															
BCF	34,991.5800	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	34,991.5800	29,228.5260	0.0000	29,228.5260	0.0000	29,228.5260	0.0000	29,228.5260	0.0000	29,228.5260	37,022.7996	37,022.7996	37,022.7996	37,022.7996	37,022.7996
Region Six Milestone															
BCF	22,148.7400	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	22,148.7400	18,500.8860	0.0000	18,500.8860	0.0000	18,500.8860	0.0000	18,500.8860	0.0000	18,500.8860	23,434.4556	23,434.4556	23,434.4556	23,434.4556	23,434.4556
Region Seven Milestone															
BCF	12,237.7300	0.0135		0.0135		0.0135		0.0135		0.0135	0.0171	0.0171	0.0171	0.0171	0.0171
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	12,237.7300	10,222.2000	0.0000	10,222.2000	0.0000	10,222.2000	0.0000	10,222.2000	0.0000	10,222.2000	12,948.1200	12,948.1200	12,948.1200	12,948.1200	12,948.1200
BCF Total	**374,165.8600**	**312,541.4160**	**0.0000**	**312,541.4160**	**0.0000**	**312,541.4160**	**0.0000**	**312,541.4160**	**0.0000**	**312,541.4160**	**395,885.7936**	**395,885.7936**	**395,885.7936**	**395,885.7936**	**395,885.7936**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Hamilton NG911, Inc.														
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	150,799.3100	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	150,799.3100	103,569.5268	0.0000	103,569.5268	0.0000	103,569.5268	0.0000	103,569.5268	0.0000	103,569.5268	136,537.6044	136,537.6044	136,537.6044	136,537.6044	136,537.6044
Region Two Milestone															
ESRP & PRF	297,968.0300	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	297,968.0300	204,645.5496	0.0000	204,645.5496	0.0000	204,645.5496	0.0000	204,645.5496	0.0000	204,645.5496	269,787.9768	269,787.9768	269,787.9768	269,787.9768	269,787.9768
Region Three Milestone															
ESRP & PRF	449,172.8800	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	449,172.8800	308,493.5976	0.0000	308,493.5976	0.0000	308,493.5976	0.0000	308,493.5976	0.0000	308,493.5976	406,692.7608	406,692.7608	406,692.7608	406,692.7608	406,692.7608
Region Four Milestone															
ESRP & PRF	16,423.1900	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	16,423.1900	11,279.5092	0.0000	11,279.5092	0.0000	11,279.5092	0.0000	11,279.5092	0.0000	11,279.5092	14,869.9836	14,869.9836	14,869.9836	14,869.9836	14,869.9836
Region Five Milestone															
ESRP & PRF	104,974.7300	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	104,974.7300	72,097.0308	0.0000	72,097.0308	0.0000	72,097.0308	0.0000	72,097.0308	0.0000	72,097.0308	95,046.8364	95,046.8364	95,046.8364	95,046.8364	95,046.8364
Region Six Milestone															
ESRP & PRF	66,446.2300	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	66,446.2300	45,635.5188	0.0000	45,635.5188	0.0000	45,635.5188	0.0000	45,635.5188	0.0000	45,635.5188	60,162.1404	60,162.1404	60,162.1404	60,162.1404	60,162.1404
Region Seven Milestone															
ESRP & PRF	36,713.2000	0.0333		0.0333		0.0333		0.0333		0.0333	0.0439	0.0439	0.0439	0.0439	0.0439
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	36,713.2000	25,214.7600	0.0000	25,214.7600	0.0000	25,214.7600	0.0000	25,214.7600	0.0000	25,214.7600	33,241.0800	33,241.0800	33,241.0800	33,241.0800	33,241.0800
ESRP & PRF Total	**1,122,497.5700**	**770,935.4928**	**0.0000**	**770,935.4928**	**0.0000**	**770,935.4928**	**0.0000**	**770,935.4928**	**0.0000**	**770,935.4928**	**1,016,338.3824**	**1,016,338.3824**	**1,016,338.3824**	**1,016,338.3824**	**1,016,338.3824**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Hamilton NG911, Inc.														
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	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	38,723.0800	30,790.9404	0.0000	30,790.9404	0.0000	30,790.9404	0.0000	30,790.9404	0.0000	30,790.9404	38,566.4304	38,566.4304	38,566.4304	38,566.4304	38,566.4304
Region Two Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	38,723.0800	60,840.5688	0.0000	60,840.5688	0.0000	60,840.5688	0.0000	60,840.5688	0.0000	60,840.5688	76,204.3488	76,204.3488	76,204.3488	76,204.3488	76,204.3488
Region Three Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	38,723.0800	91,714.3128	0.0000	91,714.3128	0.0000	91,714.3128	0.0000	91,714.3128	0.0000	91,714.3128	114,874.4928	114,874.4928	114,874.4928	114,874.4928	114,874.4928
Region Four Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	38,723.0800	3,353.3676	0.0000	3,353.3676	0.0000	3,353.3676	0.0000	3,353.3676	0.0000	3,353.3676	4,200.1776	4,200.1776	4,200.1776	4,200.1776	4,200.1776
Region Five Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	38,723.0800	21,434.2524	0.0000	21,434.2524	0.0000	21,434.2524	0.0000	21,434.2524	0.0000	21,434.2524	26,846.9424	26,846.9424	26,846.9424	26,846.9424	26,846.9424
Region Six Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	38,723.0800	13,567.3164	0.0000	13,567.3164	0.0000	13,567.3164	0.0000	13,567.3164	0.0000	13,567.3164	16,993.4064	16,993.4064	16,993.4064	16,993.4064	16,993.4064
Region Seven Milestone															
ECRF/LVF	38,723.0800	0.0099		0.0099		0.0099		0.0099		0.0099	0.0124	0.0124	0.0124	0.0124	0.0124
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	38,723.0800	7,496.2800	0.0000	7,496.2800	0.0000	7,496.2800	0.0000	7,496.2800	0.0000	7,496.2800	9,389.2800	9,389.2800	9,389.2800	9,389.2800	9,389.2800
ECRF & LVF Total	**271,061.5600**	**229,197.0384**	**0.0000**	**229,197.0384**	**0.0000**	**229,197.0384**	**0.0000**	**229,197.0384**	**0.0000**	**229,197.0384**	**287,075.0784**	**287,075.0784**	**287,075.0784**	**287,075.0784**	**287,075.0784**

Bidder Name:	Hamilton NG911, Inc.														
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															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	9,680.7700	7,775.4900	0.0000	7,775.4900	0.0000	7,775.4900	0.0000	7,775.4900	0.0000	7,775.4900	9,641.6076	9,641.6076	9,641.6076	9,641.6076	9,641.6076
Region Two Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	9,680.7700	15,363.7800	0.0000	15,363.7800	0.0000	15,363.7800	0.0000	15,363.7800	0.0000	15,363.7800	19,051.0872	19,051.0872	19,051.0872	19,051.0872	19,051.0872
Region Three Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	9,680.7700	23,160.1800	0.0000	23,160.1800	0.0000	23,160.1800	0.0000	23,160.1800	0.0000	23,160.1800	28,718.6232	28,718.6232	28,718.6232	28,718.6232	28,718.6232
Region Four Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	9,680.7700	846.8100	0.0000	846.8100	0.0000	846.8100	0.0000	846.8100	0.0000	846.8100	1,050.0444	1,050.0444	1,050.0444	1,050.0444	1,050.0444
Region Five Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	9,680.7700	5,412.6900	0.0000	5,412.6900	0.0000	5,412.6900	0.0000	5,412.6900	0.0000	5,412.6900	6,711.7356	6,711.7356	6,711.7356	6,711.7356	6,711.7356
Region Six Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	9,680.7700	3,426.0900	0.0000	3,426.0900	0.0000	3,426.0900	0.0000	3,426.0900	0.0000	3,426.0900	4,248.3516	4,248.3516	4,248.3516	4,248.3516	4,248.3516
Region Seven Milestone															
Spatial Interface	9,680.7700	0.0025		0.0025		0.0025		0.0025		0.0025	0.0031	0.0031	0.0031	0.0031	0.0031
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	9,680.7700	1,893.0000	0.0000	1,893.0000	0.0000	1,893.0000	0.0000	1,893.0000	0.0000	1,893.0000	2,347.3200	2,347.3200	2,347.3200	2,347.3200	2,347.3200
SI Total	**67,765.3900**	**57,878.0400**	**0.0000**	**57,878.0400**	**0.0000**	**57,878.0400**	**0.0000**	**57,878.0400**	**0.0000**	**57,878.0400**	**71,768.7696**	**71,768.7696**	**71,768.7696**	**71,768.7696**	**71,768.7696**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Hamilton NG911, Inc.
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/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	34,377.9400	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	27,369.7248	27,369.7248	27,369.7248	27,369.7248	27,369.7248
Region Two Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	34,377.9400	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	54,080.5056	54,080.5056	54,080.5056	54,080.5056	54,080.5056
Region Three Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	34,377.9400	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	81,523.8336	81,523.8336	81,523.8336	81,523.8336	81,523.8336
Region Four Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	34,377.9400	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	2,980.7712	2,980.7712	2,980.7712	2,980.7712	2,980.7712
Region Five Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	34,377.9400	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	19,052.6688	19,052.6688	19,052.6688	19,052.6688	19,052.6688
Region Six Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	34,377.9400	8,907.8340	0.0000	8,907.8340	0.0000	8,907.8340	0.0000	8,907.8340	0.0000	8,907.8340	12,059.8368	12,059.8368	12,059.8368	12,059.8368	12,059.8368
Region Seven Milestone															
LDB/MCS	34,377.9400	0.0065		0.0065		0.0065		0.0065		0.0065	0.0088	0.0088	0.0088	0.0088	0.0088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	34,377.9400	4,921.8000	0.0000	4,921.8000	0.0000	4,921.8000	0.0000	4,921.8000	0.0000	4,921.8000	6,663.3600	6,663.3600	6,663.3600	6,663.3600	6,663.3600
LDB Total	**240,645.5800**	**150,482.9040**	**0.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**203,730.7008**	**203,730.7008**	**203,730.7008**	**203,730.7008**	**203,730.7008**

Bidder Name:	Hamilton NG911, Inc.
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															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	34,834.1952	0.0000	34,834.1952	0.0000	34,834.1952	0.0000	34,834.1952	0.0000	34,834.1952	35,767.2540	35,767.2540	35,767.2540	35,767.2540	35,767.2540
Region Two Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	68,829.7344	0.0000	68,829.7344	0.0000	68,829.7344	0.0000	68,829.7344	0.0000	68,829.7344	70,673.3880	70,673.3880	70,673.3880	70,673.3880	70,673.3880
Region Three Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	103,757.6064	0.0000	103,757.6064	0.0000	103,757.6064	0.0000	103,757.6064	0.0000	103,757.6064	106,536.8280	106,536.8280	106,536.8280	106,536.8280	106,536.8280
Region Four Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	3,793.7088	0.0000	3,793.7088	0.0000	3,793.7088	0.0000	3,793.7088	0.0000	3,793.7088	3,895.3260	3,895.3260	3,895.3260	3,895.3260	3,895.3260
Region Five Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	24,248.8512	0.0000	24,248.8512	0.0000	24,248.8512	0.0000	24,248.8512	0.0000	24,248.8512	24,898.3740	24,898.3740	24,898.3740	24,898.3740	24,898.3740
Region Six Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	15,348.8832	0.0000	15,348.8832	0.0000	15,348.8832	0.0000	15,348.8832	0.0000	15,348.8832	15,760.0140	15,760.0140	15,760.0140	15,760.0140	15,760.0140
Region Seven Milestone															
Host Site MEVO+ (10 seats)		0.0022		0.0022		0.0022		0.0022		0.0022	0.0023	0.0023	0.0023	0.0023	0.0023
NOC/SOC		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
Text For 9-1-1		0.0042		0.0042		0.0042		0.0042		0.0042	0.0043	0.0043	0.0043	0.0043	0.0043
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	8,480.6400	0.0000	8,480.6400	0.0000	8,480.6400	0.0000	8,480.6400	0.0000	8,480.6400	8,707.8000	8,707.8000	8,707.8000	8,707.8000	8,707.8000
MISC Total	**0.0000**	**259,293.6192**	**0.0000**	**259,293.6192**	**0.0000**	**259,293.6192**	**0.0000**	**259,293.6192**	**0.0000**	**259,293.6192**	**266,238.9840**	**266,238.9840**	**266,238.9840**	**266,238.9840**	**266,238.9840**

Bidder Name:	Hamilton NG911, Inc.
Date (MM/DD/YYYY):	6/3/2020

Optional Svc for NGCS	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															
500 Mbps Primary Circuit w/ Edge Hardware - Buffalo Host		0.0026		0.0026		0.0026		0.0026		0.0026	0.0026	0.0026	0.0026	0.0026	0.0026
1000 Mbps Primary Circuit w/ Edge Hardware - Buffalo Host		0.0033		0.0033		0.0033		0.0033		0.0033	0.0034	0.0034	0.0034	0.0034	0.0034
500 Mbps Primary Circuit w/ Edge Hardware - Dawson Host		0.0026		0.0026		0.0026		0.0026		0.0026	0.0026	0.0026	0.0026	0.0026	0.0026
1000 Mbps Primary Circuit w/ Edge Hardware - Dawson Host		0.0033		0.0033		0.0033		0.0033		0.0033	0.0034	0.0034	0.0034	0.0034	0.0034
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	14,261.6188	0.0049		0.0049		0.0049		0.0049		0.0049	0.0060	0.0060	0.0060	0.0060	0.0060
NRC/MRC Region 1 Total	14,261.6188	83,768.9878	0.0000	83,768.9878	0.0000	83,768.9878	0.0000	83,768.9878	0.0000	83,768.9878	88,229.3299	88,229.3299	88,229.3299	88,229.3299	88,229.3299
Region Two Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68508 Host		0.0013		0.0013		0.0013		0.0013		0.0013	0.0013	0.0013	0.0013	0.0013	0.0013
1000 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68508 Host		0.0017		0.0017		0.0017		0.0017		0.0017	0.0017	0.0017	0.0017	0.0017	0.0017
500 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68512 Host		0.0013		0.0013		0.0013		0.0013		0.0013	0.0013	0.0013	0.0013	0.0013	0.0013
1000 Mbps Primary Circuit w/ Edge Hardware - Lincoln 68512 Host		0.0017		0.0017		0.0017		0.0017		0.0017	0.0017	0.0017	0.0017	0.0017	0.0017
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	24,769.5477	0.0153		0.0153		0.0153		0.0153		0.0153	0.0164	0.0164	0.0164	0.0164	0.0164
NRC/MRC Region 2 Total	24,769.5477	193,701.3682	0.0000	193,701.3682	0.0000	193,701.3682	0.0000	193,701.3682	0.0000	193,701.3682	201,866.3398	201,866.3398	201,866.3398	201,866.3398	201,866.3398
Region Three Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - Douglas Host		0.0016		0.0016		0.0016		0.0016		0.0016	0.0017	0.0017	0.0017	0.0017	0.0017
1000 Mbps Primary Circuit w/ Edge Hardware - Douglas Host		0.0020		0.0020		0.0020		0.0020		0.0020	0.0021	0.0021	0.0021	0.0021	0.0021
500 Mbps Primary Circuit w/ Edge Hardware - Pottawatomie Host		0.0009		0.0009		0.0009		0.0009		0.0009	0.0009	0.0009	0.0009	0.0009	0.0009
1000 Mbps Primary Circuit w/ Edge Hardware - Pottawatomie Host		0.0011		0.0011		0.0011		0.0011		0.0011	0.0011	0.0011	0.0011	0.0011	0.0011
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	4,254.3275	0.0017		0.0017		0.0017		0.0017		0.0017	0.0018	0.0018	0.0018	0.0018	0.0018
NRC/MRC Region 3 Total	4,254.3275	162,254.1997	0.0000	162,254.1997	0.0000	162,254.1997	0.0000	162,254.1997	0.0000	162,254.1997	167,145.3485	167,145.3485	167,145.3485	167,145.3485	167,145.3485
Region Four Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - Boyd Host		0.0237		0.0237		0.0237		0.0237		0.0237	0.0242	0.0242	0.0242	0.0242	0.0242
1000 Mbps Primary Circuit w/ Edge Hardware - Boyd Host		0.0307		0.0307		0.0307		0.0307		0.0307	0.0313	0.0313	0.0313	0.0313	0.0313
500 Mbps Primary Circuit w/ Edge Hardware - Cherry Host		0.0237		0.0237		0.0237		0.0237		0.0237	0.0242	0.0242	0.0242	0.0242	0.0242
1000 Mbps Primary Circuit w/ Edge Hardware - Cherry Host		0.0307		0.0307		0.0307		0.0307		0.0307	0.0313	0.0313	0.0313	0.0313	0.0313
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	5,254.1465	0.0298		0.0298		0.0298		0.0298		0.0298	0.0336	0.0336	0.0336	0.0336	0.0336
NRC/MRC Region 4 Total	5,254.1465	50,414.7955	0.0000	50,414.7955	0.0000	50,414.7955	0.0000	50,414.7955	0.0000	50,414.7955	52,501.7118	52,501.7118	52,501.7118	52,501.7118	52,501.7118
Region Five Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - Columbus Host		0.0048		0.0048		0.0048		0.0048		0.0048	0.0049	0.0049	0.0049	0.0049	0.0049
1000 Mbps Primary Circuit w/ Edge Hardware - Columbus Host		0.0058		0.0058		0.0058		0.0058		0.0058	0.0059	0.0059	0.0059	0.0059	0.0059
500 Mbps Primary Circuit w/ Edge Hardware - Saunders Host		0.0064		0.0064		0.0064		0.0064		0.0064	0.0066	0.0066	0.0066	0.0066	0.0066
1000 Mbps Primary Circuit w/ Edge Hardware - Saunders Host		0.0088		0.0088		0.0088		0.0088		0.0088	0.0089	0.0089	0.0089	0.0089	0.0089
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	13,760.9812	0.0127		0.0127		0.0127		0.0127		0.0127	0.0142	0.0142	0.0142	0.0142	0.0142
NRC/MRC Region 5 Total	13,760.9812	105,375.0432	0.0000	105,375.0432	0.0000	105,375.0432	0.0000	105,375.0432	0.0000	105,375.0432	110,246.4827	110,246.4827	110,246.4827	110,246.4827	110,246.4827
Region Six Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - First Host		0.0076		0.0076		0.0076		0.0076		0.0076	0.0077	0.0077	0.0077	0.0077	0.0077
1000 Mbps Primary Circuit w/ Edge Hardware - First Host		0.0092		0.0092		0.0092		0.0092		0.0092	0.0094	0.0094	0.0094	0.0094	0.0094
500 Mbps Primary Circuit w/ Edge Hardware - Second Host		0.0111		0.0111		0.0111		0.0111		0.0111	0.0114	0.0114	0.0114	0.0114	0.0114
1000 Mbps Primary Circuit w/ Edge Hardware - Second Host		0.0132		0.0132		0.0132		0.0132		0.0132	0.0135	0.0135	0.0135	0.0135	0.0135
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	7,505.9236	0.0105		0.0105		0.0105		0.0105		0.0105	0.0119	0.0119	0.0119	0.0119	0.0119
NRC/MRC Region 6 Total	7,505.9236	84,741.4232	0.0000	84,741.4232	0.0000	84,741.4232	0.0000	84,741.4232	0.0000	84,741.4232	88,068.8724	88,068.8724	88,068.8724	88,068.8724	88,068.8724
Region Seven Milestone															
500 Mbps Primary Circuit w/ Edge Hardware - Schuyler Host		0.0186		0.0186		0.0186		0.0186		0.0186	0.0190	0.0190	0.0190	0.0190	0.0190
1000 Mbps Primary Circuit w/ Edge Hardware - Schuyler Host		0.0232		0.0232		0.0232		0.0232		0.0232	0.0236	0.0236	0.0236	0.0236	0.0236
500 Mbps Primary Circuit w/ Edge Hardware - Fremont Host		0.0200		0.0200		0.0200		0.0200		0.0200	0.0204	0.0204	0.0204	0.0204	0.0204
1000 Mbps Primary Circuit w/ Edge Hardware - Fremont Host		0.0245		0.0245		0.0245		0.0245		0.0245	0.0250	0.0250	0.0250	0.0250	0.0250
Tier 3 Logix		0.0102		0.0102		0.0102		0.0102		0.0102	0.0104	0.0104	0.0104	0.0104	0.0104
GeoComm GIS Data Hub Aggregation & QA/QC	3,002.3694	0.0076		0.0076		0.0076		0.0076		0.0076	0.0086	0.0086	0.0086	0.0086	0.0086

NRC/MRC Region 7 Total	3,002.3694	78,845.0226	0.0000	78,845.0226	0.0000	78,845.0226	0.0000	78,845.0226	0.0000	78,845.0226	81,011.6904	81,011.6904	81,011.6904	81,011.6904	81,011.6904
Opt. Svc NGCS Total	**72,808.9148**	**759,100.8401**	**0.0000**	**759,100.8401**	**0.0000**	**759,100.8401**	**0.0000**	**759,100.8401**	**0.0000**	**759,100.8401**	**789,069.7755**	**789,069.7755**	**789,069.7755**	**789,069.7755**	**789,069.7755**