**DEVELOPMENT AGREEMENT**
**BETWEEN**
**CITY OF JOPLIN AND ALLO MISSOURI, LLC**

| CITY | | ISP | |
|---|---|---|---|
| **CITY OF JOPLIN**<br>**602 S. MAIN STREET**<br>**JOPLIN, MO 64801** | | Name: ALLO Missouri, LLC<br>Address: 330 S. 21st Street<br>Lincoln, Nebraska 68510 | |
| Attention: Troy Bolander | | Attention: Bradley A. Moline, President and CEO | |
| Department: Planning, Development & NS | | Phone: (402) 480-6550 | Fax: N/A |
| Phone: (417) 624-0820 | Fax: | | |

**WHEREAS**, the City has identified significant broadband gaps and desired improved broadband connectivity and

**WHEREAS,** ALLO Missouri, LLC ("ISP") has been selected by the City of Joplin, Missouri (the "City") process to construct a fiber optic network intended to pass all homes, anchor institutions, and businesses in the City

**WHEREAS**, the City and ISP expect the Project (as defined below), when operational, to provide significant socio-economic and community benefits to the City over time; and

**WHEREAS**, to develop the Project, ISP will incur significant costs, including costs for items that are for a public purpose and will benefit the City; and

**WHEREAS**, the City and ISP enter into this Development Agreement (the "Agreement"), whereby ISP agrees to fund, develop, and build the Project and the City agrees to provide certain concessions, including reimbursement of certain fees and expenses.

**THIS AGREEMENT** is made and entered into this ____ day of _____, 2024, by the City and ISP ("Effective Date").

The City and ISP agree to the following:

1. **The Project**. The "Project" means the construction of a fiber optic network that is able to offer high-quality, fiber optic broadband to substantially all residents, anchor institutions, and businesses in the City (the "Network") that are accessible using public rights-of-way and similar public easements, ways and extension and additions thereto (collectively, the "ROW"). The Network facilities shall be owned and

operated by ISP and located within the corporate limits of the City, as detailed in Attachment A (the "Project Area").

2. **Period of Performance.** Promptly following the Effective Date, the Parties shall enter into the Non-Exclusive Public ROW License Agreement, the form of which is attached hereto as Exhibit E ("Non-Exclusive Public ROW License Agreement"). The ISP will make commercially reasonable efforts to construct and Substantially Complete the Network within 24 months following the date the first Network construction permit is duly issued by the City to ISP. The ISP will have until August 31, 2026, to seek reimbursement for Eligible Expenses in accordance with this Agreement. "Substantially Complete" or "Substantial Completion" means the date, as reasonably determined by ISP, that the Network is capable (but for lack of a fiber drop) of providing broadband services to substantially all passings in the City. "Passing" means a physical location (residence, business, or government entity) within the Project Area that ISP is capable of serving from its Network within ROW using a drop. ISP shall provide written notice of Substantial Completion to the City and shall provide reasonable supporting evidence to demonstrate the Network is Substantially Compete.

3. **ISP Responsibilities**. ISP agrees to the following list of responsibilities and deliverables:
   - ISP will construct a the Network intended to pass every home, anchor institution, and business identified in the map on Attachment A. This obligation is subject to the buildout requirements included in the Non-Exclusive Public ROW License Agreement, and shall exclude areas in which ISP is unable to obtain access through the ROW or other private property access right. After the Network identified in Attachment A is completed, ISP shall have the right, but not the obligation, to extend its facilities to additional portions of the City.
   - ISP will offer discounted broadband option for low-income households, which may be satisfied by ISP's participation in the FCC's Affordable Connectivity Program or any successor plan ("ACP Plan"). To the extent that the ACP Plan is no longer active, ISP will coordinate with the City to develop a low-income plan and agrees to make commercially reasonable efforts to provide discounted broadband to qualifying households in the City.
   - ISP will operate a customer service line and online services that are substantially similar to ISP's customer service practices in existing markets and are intended to meet the needs of the City's citizens. In addition, the ISP will operate a local business office that will be open to the public during regular business hours.
   - ISP will provide the name and contact information for the local ISP primary point of contact and will keep the City updated should the contact person change.
   - ISP agrees to make its commercially reasonable efforts to meet the construction schedule included in Attachment B.
   - To the extent that the City contributes funding derived from the American Rescue Plan Act of 2021 ("ARPA") to fund construction of the Network, ISP shall adhere with applicable ARPA rules and reporting requirements as detailed in Attachment C.
   - ISP will have diverse backhaul circuits into the City and will place two Central Offices (each, a "CO") within the City. Each CO will serve approximately half the city. ISP will install a diverse fiber optic ring between the COs. These enhancements are expected to increase reliability of services to the residents and businesses in the City. If one CO is rendered wholly or partially inoperable, , it is expected the alternate CO will continue to operate providing services to its service area (approximately half the City) as well as any institutions or businesses with redundant fiber connections to both COs. Each CO will be equipped with battery backup and a backup generator to ensure operation during power events.
   - ISP will maintain a disaster recovery plan. ISP's current Disaster Recovery Plan is included as Attachment D ("Disaster Recovery Plan"). ISP will test the Disaster Recovery Plan with City officials present a minimum of twice per year and report the results of the test to the City. The Disaster Recovery Plan will include a description of the storage of spare electronics and fiber needed to restore the network after an outage.

- ISP will construct the Network in accordance with its current processes and procedures and prevailing industry standards as they are in effect from time to time. However, ISP will reasonably cooperate with the City to ensure that at least some of the early construction is within low to moderate income neighborhoods.
- ISP will provide a written description of its processes used to log problems reported by customers and a description of how ISP confirms all problems are addressed and resolved.
- ISP shall not increase retail prices for its 1 Gig residential broadband service tier for a period of 36 months following the Effective Date (it being understood and acknowledged that the foregoing shall not prohibit ISP's ability to passthrough any governmental fees, charges, or other expenses to its customers located in the City).

4. **Technical Requirements**. The Network will meet the following technical requirements.
   - ISP will initially utilize XGS-PON electronics technology that is capable of delivering up to 10-gigabits of upload and download speed to residents and businesses.
   - The Network will consist of a minimum of 30% buried fiber, with the percentage measured in terms of route miles.
   - Buried fiber must be located inside of a conduit that includes a locating wire or is otherwise discoverable by the locating equipment used to identify buried utilities. All conduit must be buried to a depth of at least 36 inches below street level unless alternate depths are agreed upon by City and ISP or otherwise permitted by applicable law. Notwithstanding the foregoing, fiber drops shall not be subject to the burial depth requirements found in this Section 4.
   - For aerial fiber construction, ISP shall execute a pole attachment agreement with the pole owner(s) in the City to the extent such agreement is required by the applicable pole owner. Copies of the executed pole attachment agreement(s) shall be provided to the City before starting any make-ready or fiber construction on poles. If the ISP requires additional poles to be installed to meet the Network's final design, the ISP will seek approval from the City prior to installing the new poles, and the City's approval shall not be unreasonably withheld, conditioned, or delayed.
   - ISP shall obtain all permits, ROW authority, and easements from the appropriate government entity for public rights-of-way necessary to Substantially Complete the Network. These may include, but are not limited to, all authorities having jurisdiction (local, state, and federal), railroad crossings, water crossings, wetland crossings, and road crossings. ISP shall use commercially reasonable efforts to obtain private right-of-way, private easements, and other rights of access with private parties required for the construction of the Network. Upon request, the, ISP will provide the City with electronic copies of the aforementioned documents for inclusion in the project records and archives.
   - ISP shall adhere to national standards related to fiber construction and fiber electronics as each are applicable and in effect from time to time, including:
     - National Electrical Code, NFPA 70
     - ANSI/TIA/EIA Standards
     - Fiber Optic Test Standards, TIA/EIA-526
     - Customer-owned Outside Plant. ANSI/TIA/EIA-758
     - National Electric Safety Code
   - ISP shall follow applicable State and local requirements for the safe locating of existing underground utilities and other impediments.
   - ISP shall allow for inspection by the City of the construction process to make sure that the Network meets the design specifications outlined in this Agreement.
   - ISP shall adhere to all City requirements related to construction of the Network including:
     - Applying for all necessary permits;
     - Maintaining compliance with applicable Missouri 811 laws;
     - The ISP agrees that during construction of the Network, adequate barricades, guards and warning signs, lights or devices consistent with the requirements contained in the Manual on Uniform Traffic Control Devices shall be provided by ISP during construction;
     - Notification to the public for scheduled construction;
     - Safety rules for routing traffic around construction zones;

    - Rules associated with maintaining a neat worksite and mitigating mud and runoff;
    - Inspection of work site before, during, or after construction, as required;
    - To the extent possible, return construction areas to the condition present before construction.
  - ISP shall use commercially reasonable efforts to construct the Network in a manner that is safe for the public and for contractors working on the Network.
  - ISP shall maintain a log of all complaints from residents related to the construction process. The log should include the resolution of the complaint. Upon request, ISP shall share the log with the City during the Network construction process.
  - ISP shall provide a written description of the process by which the public may notify ISP about damage caused during Network construction. This process of logging problems from the public and resolving each issue is included in Attachment E.
  - ISP shall provide a copy of final construction drawings to the City in an electronic format to be agreed upon by the parties.

**5. Responsibilities of the City**. The City shall make commercially reasonable efforts to remove barriers that may delay the construction of the Network, and will reasonably cooperate with ISP to remove such barriers as they are identified. The City agrees to work with ISP to clear administrative hurdles as they occur during the construction process by taking certain steps including, but not limited to, the following:

- The City shall pay all Eligible Expenses in accordance with this Agreement;
- City will review and approve construction in ROW; City permits shall not be required for ISP's drops;
- City will offer an efficient, documented permitting process that describes the needed detail to be provided by ISP, the cost, and the expected turnaround time to approve permit requests;
- City will strive to provide locations on City-owned or controlled land for the placement of the ISP COs and fiber distribution cabinets. City shall provide a location for ISP to store fiber and other construction materials during the construction process;
- City will make all GIS data, parcel data, and data concerning the location of other utilities available to ISP. Such data will be provided in GIS format (e.g., geodatabase (.gdb) or shapefiles (.shp)) when possible. City will keep ISP informed of changes from other utilities during the construction process;
- City will provide updated list of addresses of residents, business, and anchor institution locations when requested by ISP;
- City will provide contact information for homeowner associations, private developers, or any other entities that ISP may need to coordinate with during construction; and
- City will provide sufficient staff to be able to meet its permitting and locating obligations in a timely manner and at a reasonable nominal cost to the ISP.

**6. City Contribution; Reimbursement**. The City shall contribute up to $5,000,000 to the ISP's construction of the Network in the form of cash reimbursement to the ISP ("Aggregate City Reimbursement") toward the following construction requirements, which are designed to benefit the City by adding additional resiliency features to the Network:

a. Construction of an additional and redundant CO to allow for redundancy of the Network in the event the primary CO is unable to serve the Network. The location of such CO is to be mutually agreed upon by the ISP and the City prior to the construction of the Network.
b. A fiber drop to the City's anchor institutions will be installed to add additional security and protection of their connections. Anchor institutions shall include city hall, public works operations facility, public schools, police stations, fire stations, hospitals, and similar Passings within the Project Area that serve a public purpose.
c. Mainline Fiber will be buried to ensure the main backbone of the Network is protected. "Mainline Fiber" means primary and backbone fiber optic cables that form the core of the Network. Prior to construction, the ISP will reasonably coordinate with the City to identify Mainline Fiber routes, and will identify in a final construction map the Mainline Fiber routes that will be buried prior to construction permits being issued.
d. The activities undertaken by ISP in accordance with Section 6.a, 6.b, and 6.c are collectively referred to as the "Reimbursable Activities". All costs and expenses for materials, labor, subcontractor costs and expenses, permitting expense charged by entities other than the City, and all other costs and expenses

which are related to, or arise from, the Reimbursable Activities shall be collectively referred to as the "Eligible Expenses."

e. The ISP will have until August 31, 2026 to submit Reimbursement Requests for Eligible Expenses in accordance with the procedures in this Section 6.e. Commencing after any Eligible Expenses have been incurred by ISP, ISP shall have the right to periodically submit requests for reimbursement (each, a "Reimbursement Request") to the City. Reimbursement Requests shall not be submitted more frequently than monthly and collectively shall not exceed the Aggregate City Reimbursement. Each Reimbursement Request shall be accompanied by cost breakdowns for Eligible Expenses. Upon receipt of a Reimbursement Request, the City shall promptly review the Reimbursement Request and shall promptly inform ISP of any disputes relating to the applicable Reimbursement Request. The City shall pay all undisputed amounts associated with Reimbursement Requests within thirty (30) calendar days of its receipt of the applicable Reimbursement Request. All disputes associated with Reimbursement Request shall be resolved by ISP and City in accordance with Section 33 of this Agreement. If the City fails to pay any amounts detailed within a Reimbursement Request and such Reimbursement Request is not disputed by the City within fourteen (14) calendar days of receipt of the applicable Reimbursement Request, then, in addition to any other remedies at law or equity, ISP shall have the right to offset unpaid amounts of Reimbursement Requests on a dollar for dollar basis against any fees payable to the City under the Non-Exclusive Public ROW License Agreement or any successor agreement.

**7. Working Relationship Between ISP and City**.

- The City and ISP will work together after signing this Agreement to develop a reporting process for the parties to regularly communicate on the Project.
- ISP agrees to regularly report to City Council on the progress of the Project.

Each party shall designate a specific single point of contact for all correspondence between the two parties, along with alternate contact if the primary contact is not available.

**8. Insurance Requirements**. Without limiting any of the other obligations or liabilities of the ISP, the ISP shall secure and maintain at its own cost and expense, throughout the duration of this Agreement and until the work is Substantially Complete, insurance in accordance with this Section 8. After Substantial Completion, ISP shall maintain insurance in accordance with the Non-Exclusive Public ROW License Agreement. The form and limits of such insurance, together with the underwriter thereof in each case, are subject to approval by the City of Joplin. Regardless of such approval, it shall be the responsibility of the ISP to maintain adequate insurance coverage during the term of the Agreement. Failure of the ISP to maintain coverage shall not relieve it of any contractual responsibility or obligation or liability in general.

The certificates of insurance, including evidence of the required endorsements hereunder or the policies, shall be filed with the City within ten (10) days after the date of the receipt of Notice of Award of the Contract to the ISP and prior to the start of work. All insurance policies shall require that the insurance company in question provide thirty (30) days written notice prior to modification or cancellation of such insurance. Such notices shall be mailed, certified mail, return receipt requested, to:

City of Joplin - Public Works, 602 S. Main Street, Joplin, MO 64801

Such policies shall name the City as an additional insured, with limits of liability not less than the sovereign immunity limits for Missouri public entities calculated by the Missouri Department of Insurance as of January 1 each calendar year and published annually in the Missouri Register pursuant to Section 537.610, RSMo. (See, http://insurance.mo.gov/industry/sovimmunity.php)

As of January 1, 2023, the minimum coverage for the insurance referred to herein shall be as set out below:

**a. Workers' Compensation….** Statutory coverage per RSMo 287.010 et seq

**Employer's Liability…….** $1,000,000.00

**b. Commercial General Liability Insurance**, including coverage for Premises, Operations, Products and Completed Operations, Contractual Liability, Broad Form Property Damage, Independent ISPs, Explosion, Collapse, and Underground Property Damage and endorsed for blasting if blasting required. Such coverage shall apply to bodily injury and property damage on an "Occurrence Form Basis" with limits of at least $3,370,137.00 for all claims arising out of a single accident or occurrence and at least $505,520.00 with respect to injuries and/or death of any one person in a single occurrence and an amount not less than at least $1,000,000 for all claims to property arising out of a single occurrence and at least $100,000 to any one owner with respect to damages to property. ISP agrees that the proceeds of such insurance policy shall first be used to pay any award, damages, costs, and/or attorneys' fees incurred by or assessed against City, its employees, officers and agents, before payment of any award, damages, costs or attorneys' fees of ISP, its employees, officers or agents. ISP agrees to cause its insurer to name City as an additional insured on such insurance policy, including the City as an additional insured for coverage under its products-completed operations hazard, and said policy shall be primary and noncontributory.

**c. Automobile Liability Insurance** covering bodily injury and property damage for owned, non-owned and hired vehicles, with limits of at least $3,370,137.00 for all claims arising out of a single accident or occurrence and at least $505,520.00 with respect to injuries and/or death of any one person in a single accident or occurrence.

**d. Subcontractors**. The ISP shall require subcontractors performing construction work related to the Project to maintain all insurance required in subparagraphs (a), (b) and (c) hereof and in like amounts.

**e. Notice**. The ISP and/or subcontractor shall furnish the City prior to beginning the work, the policy as specified in subparagraph (d), and satisfactory proof of carriage of all the insurance required by this Agreement, with the provision that policies shall not be canceled or non-renewed without thirty (30) days written notice to the City of Joplin.

**f. Legislative or Judicial Changes.** In the event the scope or extent of the City's tort liability as a governmental entity as described in Section 537.600 through 537.650 RSMo is broadened or increased during the term of this Agreement by legislative or judicial action, the City may require ISP, upon 30 days written notice, to execute an addendum to this Agreement whereby the ISP agrees to provide, at a price not exceeding ISP's actual increased premium cost, additional liability insurance coverage as the City may require to protect the City from increased tort liability exposure as the result of such legislative or judicial action. Any such additional insurance coverage shall be evidenced by an appropriate certificate of insurance and shall take effect within the time set forth in the addendum.

**9. Certification Regarding Disbarment, Eligibility, Indictments, Convictions or Civil Judgements for all Federal Aid Projects:** By signing and submitting the bid, the authorized official of the bidder, under penalty of perjury under the laws of the USA, shall certify that, except as noted in the exceptions, the company or any person associated therewith in the capacity of owner, partner, director, officer, principal investor, project director, manager, auditor or any position involving the administration of federal funds:

a. Is not currently under suspension, debarment, voluntary exclusion or determination of ineligibility by any federal agency.
b. Has not been suspended, debarred, voluntarily excluded or determined ineligible by any federal agency within the past three years.
c. Does not have a proposed debarment or suspension pending.
d. Has not been indicted, convicted or had a civil judgment rendered against any of the listed parties by a court of competent jurisdiction in any matter involving fraud or official misconduct within the past three years.

**9.1** If there are any exceptions, the bidder shall submit the exceptions on company letterhead, signed by the bidder and inserted inside the bid submitted. Exceptions will not necessarily result in denial of award, but will be considered in determining bidder responsibility. For any exception noted, the bidder shall indicate to whom it applies, the initiating agency, and dates of action. Providing false information may result in criminal prosecution or administrative sanctions.

**9.2** By signing the Agreement, the ISP shall further certify that all related subcontracts of $25,000 shall comply with the requirements of this Section 9.

**10. ISP's responsibility for subcontractors**. The ISP shall be as fully responsible to the City for the acts and omissions of its subcontractors, and of persons either directly or indirectly employed by them, as ISP is for the acts and omissions of persons it directly employs. ISP shall cause appropriate provisions to be inserted in all subcontract agreements relating to this work, to bind all subcontractors to ISP by all applicable terms herein set forth, and insofar as applicable to the work of subcontractors and to give ISP not less than the same power regarding termination of any subcontract as the City may exercise over ISP under any provisions of this Agreement. Nothing contained in this Agreement shall create any contractual relation between a subcontractor and the City.

**11. General Independent Contractor Clause**. This Agreement does not create an employee/employer relationship between the parties. It is the parties' intention that the ISP will be an independent contractor and not the City's employee for all purposes, including, but not limited to, the application of the Fair Labor Standards Act minimum wage and overtime payments, Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code, Missouri Revenue and Taxation laws, Missouri Workers' Compensation and Unemployment Insurance laws. The ISP will retain sole and absolute discretion in the judgment of the manner and means of carrying out the ISP's activities and responsibilities hereunder. The ISP agrees that it is a separate and independent enterprise from the City, that it has a full opportunity to find other business, that it has made its own investment in its business, and that it will utilize prevailing industry standards while performing the work. This Agreement shall not be construed as creating any joint employment relationship between the ISP and the City, and the City will not be liable for any obligation incurred by the ISP, including but not limited to unpaid minimum wages and/or overtime premiums (it being understood and acknowledged by the City that the foregoing shall not restrict ISP's right to seek reimbursement for Eligible Expenses).

**12. Reserved.**

**13. Termination; Default**.

a. A Default under this Agreement shall occur if: (1) a party materially breaches this Agreement (2) such breach is not excused by any provision of this Agreement; and (3) such breach continues un-remedied for a period of thirty (30) calendar days following receipt of written notice from the non-breaching party. If the breach by its nature cannot be cured within thirty (30) calendar days, and the breaching party within that time has diligently commenced a cure that is satisfactory to the non-breaching Party, there shall be no Default as long as the Party diligently continues such cure to completion as soon as possible, and in no event exceeding sixty (60) calendar days of the original Notice of Default. Without limiting the foregoing the following shall also constitute a Default: (4) a series of non-material or persistent breaches by ISP that, in the aggregate, have a material and significant adverse impact on the services to, or the support and operational management of, the Network; or (5) ISP becomes insolvent, is unable to pay its debts, enters into or files a petition, arrangement, application, action or other proceeding seeking relief or protection under the bankruptcy laws of the United States, or is the subject of any such proceeding initiated by another party and such proceeding is not discharged and/or dismissed within ninety (90) days of the filing date.

b. Upon the occurrence of a Default, the non-breaching party shall have the right, subject to any express limitations contained in this Agreement, to immediately terminate this Agreement and/or suspend performance under this Agreement. Unless otherwise stated in this Agreement, nothing in this Agreement shall preclude either Party from also pursuing other available remedies, including, but not limited to, damages, injunctive relief, and costs (including reasonable attorneys' fees).

**14. Liability and Indemnity**.

**a.** NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES, WHETHER FORESEEABLE OR NOT, INCLUDING WITHOUT LIMITATION AS APPLICABLE, ECONOMIC LOSS OR LOST BUSINESS OR PROFITS, INTERRUPTIONS OF SERVICE, OR ANY DELAY, ERROR OR LOSS OF DATA OR INFORMATION, ARISING IN ANY MANNER OUT OF, OR IN CONNECTION WITH, THIS AGREEMENT AND A PARTY'S PERFORMANCE OR NONPERFORMANCE OF ITS OBLIGATIONS UNDER THIS AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT (INCLUDING STRICT LIABILITY), ALL CLAIMS FOR WHICH ARE HEREBY SPECIFICALLY WAIVED. THE MAXIMUM AGGREGATE LIABILITY OF ISP FOR ANY AND ALL CLAIMS ARISING FROM, OR RELATING TO, THIS AGREEMENT, SHALL NOT EXCEED THE LESSER OF (1) THE FEES PAID AND OWED TO ISP UNDER THIS AGREEMENT; OR (2) $5,000,000. The foregoing limitations of liability shall not apply to claims arising from or relating to a party's gross negligence or willful misconduct.

**b.** Except as provided herein, each Party and subject to Section 14.a, on behalf of itself and its affiliates, directors, officers, employees, agents, successors, and assigns ("Indemnitor") agrees to indemnify, defend, protect and hold the other Party and its directors, officers, directors, employees, agents, successors, and assigns ("Indemnitee") harmless from and against any claims, suits, actions or damages brought or asserted by a third party of any kind or character (collectively "Claims") and from and against any liability, losses, fines, judgments, costs and expenses (including reasonable attorney, accountant and expert fees) arising out of any Claims (collectively, "Losses") incurred by any Indemnitee (a) because of the death of any person, or any injuries or damage received or sustained by any persons or property, which in whole or in part arises on account of the negligent acts, errors, or omissions or willful misconduct of the Indemnitor in the performance of its obligations or exercise of its rights under this Agreement, including any material violation by Indemnitor of any law or permit applicable thereto; (b) under the Workers' Compensation laws asserted by any other person providing goods or services for or on behalf of any of the foregoing in connection with this Agreement; or (c) arising out of, caused by, related to, or based upon, a contractual or other relationship between such claiming party and the Indemnitor. The Indemnitor shall defend the Indemnitee in any proceeding alleging the third party claims listed above, at Indemnitor's sole cost and expense. The Indemnitor will have the option to select and provide legal counsel for that defense. If Indemnitee wants additional counsel of its choosing, the costs and expenses of the additional counsel will be Indemnitee's responsibility, and Indemnitor will have no obligation to pay additional counsel. Indemnitor's counsel will lead, direct and manage the litigation, and will ensure Indemnitee's additional counsel receives adequate information to monitor the litigation.

**c.** The ISP shall indemnify and hold the City harmless from all wages or overtime compensation due any of ISP's employees in rendering services pursuant to this agreement or any subcontract, including payment of reasonable attorneys' fees and costs in the defense of any claim made under the Fair Labor Standards Act, the Missouri Prevailing Wage Law or any other federal or state law.

**c.** The indemnification obligations of ISP hereunder shall not be limited by any limitations as to the amount or type of damages, compensation or benefits payable by or for the ISP, under any federal or state law, to any person asserting the claim against City, its elected or appointed officials, agents and employees, for which indemnification is sought.

**d.** The indemnification obligations herein shall not negate, abridge or reduce in any way any additional indemnification rights of the City, its elected or appointed officials, agents and employees, which are otherwise available under statute, or in law or equity.

**e**. The ISP shall indemnify and hold the City harmless for any penalties, fines, fees or costs, including costs of defense, which are charged or assessed by any Federal, state or local agency including, but not limited to, Environmental Protection Agency or Department of Natural Resources directly caused by ISP's gross negligence or willful misconduct.

**15. Force Majeure Events**. Notwithstanding any other provision of this Agreement, neither party shall be responsible to the other party, or for any loss or damage, resulting from any event or circumstance beyond the reasonable control of the Party, including but not limited to an earthquake, hurricane, fire, flood, lightning, sinkhole or other forces of nature, acts of war, terrorism (including cyberterrorism), or civil unrest, strikes, lockouts or other labor unrest, unforeseeable inflation or supply chain issues, pandemics or legal order, government action or application of laws, regulations or codes (each a, "Force Majeure Event"). A party whose performance is impacted by a Force Majeure Event shall provide reasonable notice to the other party and shall make commercially reasonable efforts to minimize the impact of the Force Majeure Event on its performance. The deadline by when a party must perform an obligation under this Agreement, shall be postponed by the period of time by which the party's ability to perform that obligation is materially prevented or interfered with by a Force Majeure Event.

**16. Confidentiality**. The City agrees to keep confidential any and all Confidential Information, to the fullest extent permitted by law. In the event a public records request is made for Confidential Information and/or documents designated as confidential or proprietary, the City shall notify ISP as soon as possible. For all purposes of this Agreement, the term "Confidential Information" shall collectively refer to all non-public information or material disclosed or provided by one party to the other either orally or in writing including without limitation: (a) business plans, strategies, forecasts, projects and analyses, (b), financial information and fee structures, (c) business processes, methods and models, (d) employee information, (e) specifications, (f) manufacturing, purchasing, logistics, sales, technical, product and marketing information, and (g) customer information or personal data.

**17. Hierarchy of Documents**. In the event of a conflict between this Agreement and the Non-Exclusive Public ROW License Agreement , the order of precedence set forth below shall control:

a. Non-Exclusive Public ROW License Agreement
b. This Agreement

**18. Conflict of Interest**. In accepting this contract, ISP certifies that no member or officer of its firm or corporation is an officer or employee of the City of Joplin, Missouri, or any of its boards or agencies, and further that no officer or employee of the City has any financial interest, direct or indirect, in this contract. All applicable federal regulations and provisions of R.S.Mo. Section 105.450 et seq. shall not be violated.

**19. Assignment.** Except as provided for in this Section 20, ISP shall not assign any interest in this Agreement, and shall not transfer any interest in the same (whether by assignment or novation), without prior written consent of the City thereto, such consent not to be unreasonably withheld, conditioned, or delayed. No such consent shall be required for: (a) a transfer in trust, by mortgage, by other hypothecation, or by assignment of any rights, title, or interest of this Agreement or Network to secure indebtedness; or (b) an assignment or transfer to corporation, partnership, or other legal entity controlling, controlled by or under common control of the ISP, or to any successor to the ISP by purchase, merger, consolidation or reorganization.

**20. Nondiscrimination**. The ISP agrees in the performance of this contract not to discriminate on the ground or because of race, creed, color, national origin or ancestry, sex, religion, handicap, age, status as a protected veteran or status as a qualified individual with a disability, or political opinion or affiliation, against any employee of ISP or applicant for employment and shall include a similar provision in all subcontracts let or awarded hereunder. The parties hereby incorporate the requirements of 41 C.F.R. §§ 60-1.4(a)(7), 29 C.F.R. Part 471, Appendix A to Subpart A, 41 C.F.R. § 60-300.5(a)ii and 41 C.F.R. § 60-741.5(a), if applicable.

a. This ISP and its subcontractors shall abide by the requirements of 41 C.F.R. § 60-300.5(a). This regulation prohibits discriminations against qualified protected veterans and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified protected veterans.

b. This ISP and its subcontractors shall abide by the requirements of 41 C.F.R. § 60-741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

**21. Nonresident/Foreign Corporation**. ISP shall procure and maintain during the life of this contract:

a. If the ISP is a foreign corporation, a certificate of authority to transact business in the State of Missouri from the Secretary of State, unless exempt pursuant to the provisions of Section 351.570 R.S.Mo.

b. A certificate from the Missouri Director of Revenue evidencing compliance with the transient employer financial assurance law, unless exempt pursuant to the provisions of Section 285.230 RSMo.

**22. Notices**. All notices required or permitted hereinunder and required to be in writing may be given first class mail addressed to City and ISP at the addresses shown above. The date of delivery of any notice given by mail shall be the earlier of the date falling on the second full day after the day of its mailing or the date or receipt (as demonstrated by a return receipt or similar documentation).

**23. Records and Audits.** The ISP shall maintain accounts and records, including personnel, property, and financial records, adequate to identify and account for all Eligible Expenses and such other records as may be deemed necessary by the City to assure proper accounting for Eligible Expenses. These records will be made available for audit purposes to the City or any authorized representative and will be retained for three years after Substantial Completion.

**24. Authorized Employees**. ISP acknowledges that Section285.530, RSMo, prohibits any business entity or employer from knowingly employing, hiring for employment, or continuing to employ an unauthorized alien to perform work within the State of Missouri. ISP therefore covenants that is not knowingly in violation of subsection 1 or Section 285.530, RSMo, and that it will not knowingly employ, hire for employment, or continue to employ any unauthorized aliens to perform work on the Project, and that its employees are lawfully to work in the United States.

**25. Interest of Members of a City.** No member of the governing body of the City and no other officer, employee, or agent of the City who exercises any functions or responsibilities in connection with the planning and carrying out of the Project, shall have any personal financial interest, direct or indirect, in this Agreement, and the ISP shall take appropriate steps to ensure compliance.

**26. Affidavit for Contracts Over $5,000.00**. That pursuant to Missouri Revised Statute Sections 285.525 through 285.550, if this contract exceeds the amount of $5,000.00 and ISP is associated with a business entity, ISP shall provide an acceptable notarized affidavit stating that the associated business entity is enrolled in and participates in a federal work authorization program with respect to the employees working in connection with the contracted services, and that said business entity does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. Additionally, ISP must provide documentation for said business entity evidencing current enrollment in a federal work authorization program.

**27. City Benefits**. ISP shall not be entitled to any of the benefits established for the employees of the City nor be covered by the Worker's Compensation Program of the City.

**28. Occupational License**: The ISP shall obtain and maintain an occupational license with the City of Joplin, Missouri, if required by city code and any required state or federal license. The cost for this occupational license shall be borne by the ISP. No contract will be executed by the City until this occupational license has been obtained and the ISP is current on any City taxes is verified.

**29. Compliance with Laws.** ISP agrees to comply with applicable federal, state and local laws or rules and regulations applicable to the provision of services and products hereunder. ISP affirmatively states that payment of all local, state, and federal taxes and assessments owed by ISP is current.

**30. Entire Agreement**. This Agreement contains the entire agreement of the parties related to the subject matter hereto. No modification, amendment, or waiver of any of the provisions of this agreement shall be effective unless in writing signed by authorized representatives of each party.

**31. Dispute Resolution.** Except for an action seeking a temporary restraining order or an injunction or to compel compliance with this dispute resolution procedure, or any scenario where a party may be prejudiced by following the dispute resolution procedure (*e.g.*, expiration of the statute of limitations) the parties shall have the right to invoke the dispute resolution procedures in this Section at any time to resolve a controversy, claim, or breach arising under this Agreement. Each party shall bear its own costs for dispute resolution activity. At either party's written request, each party shall designate knowledgeable, responsible, senior representatives to meet and negotiate in good faith to resolve a dispute. The representatives shall have discretion to decide the format, frequency, duration, and conclusion of these discussions. The parties shall conduct any meeting in-person or via conference call, as reasonably appropriate within thirty

(30) calendar days of the initial notice of dispute. If thirty (30) calendar days after the first in-person meeting of the senior representatives, the parties have not resolved the dispute to their mutual satisfaction, each party shall designate executive representatives at the director level or above to meet and negotiate in good faith to resolve the dispute. To facilitate the negotiations, the parties may agree in writing to use mediation or another alternative dispute resolution procedure. In the case of a dispute over a payment, either party may seek to use non-binding mediation. The parties shall mutually agree on a qualified mediator, no later than fourteen (14) calendar days after a party submits a written request for mediation to the other party. Mediation shall take place in Joplin, Missouri. Arrangements reached in mediation shall be enforceable as settlement agreements in any court having jurisdiction thereof. If after sixty (60) days from the first executive-level, in-person meeting, the parties have not resolved the dispute to their mutual satisfaction either party may invoke any legal means available to resolve the dispute. Unless the parties otherwise agree in writing, communication between the Parties under this Section shall be treated as confidential information developed for settlement purposes, exempt from discovery, and inadmissible in litigation. During any dispute resolution procedure or lawsuit, the Parties shall continue providing services to each other and performing their obligations under this Agreement that are not subject to any dispute.

**32. Jurisdiction**. This Agreement and every question arising hereunder shall be construed or determined according to the laws of the State of Missouri. Should any part of this agreement be adjudicated, venue shall be proper only in the Circuit Court of Jasper County, Missouri.

**33. Attachments**. The following Attachments are attached hereto and incorporated into this Agreement by reference.

Attachment A – Project Area
Attachment B – Network Construction Schedule
Attachment C – Government Funding Requirements
Attachment D – Disaster Recovery Plan
Attachment E – Form of Non-Exclusive Public ROW License Agreement (Will be presented to City Council at a future date)

**IN WITNESS WHEREOF,** the parties hereto have set their hands and seals on the day and year herein stated.

**CERTIFICATE OF DIRECTOR OF FINANCE**

I certify that the expenditure contemplated by this document is within the purpose of the appropriation to which it is to be charged and that there is an unencumbered balance of appropriated and available funds to pay therefor.

_____
Leslie Haase, Director of Finance

**APPROVED AS TO FORM**

_____
Peter Edwards, City Attorney

President & CEO

**ISP**: ALLO Missouri, LLC

By:_____

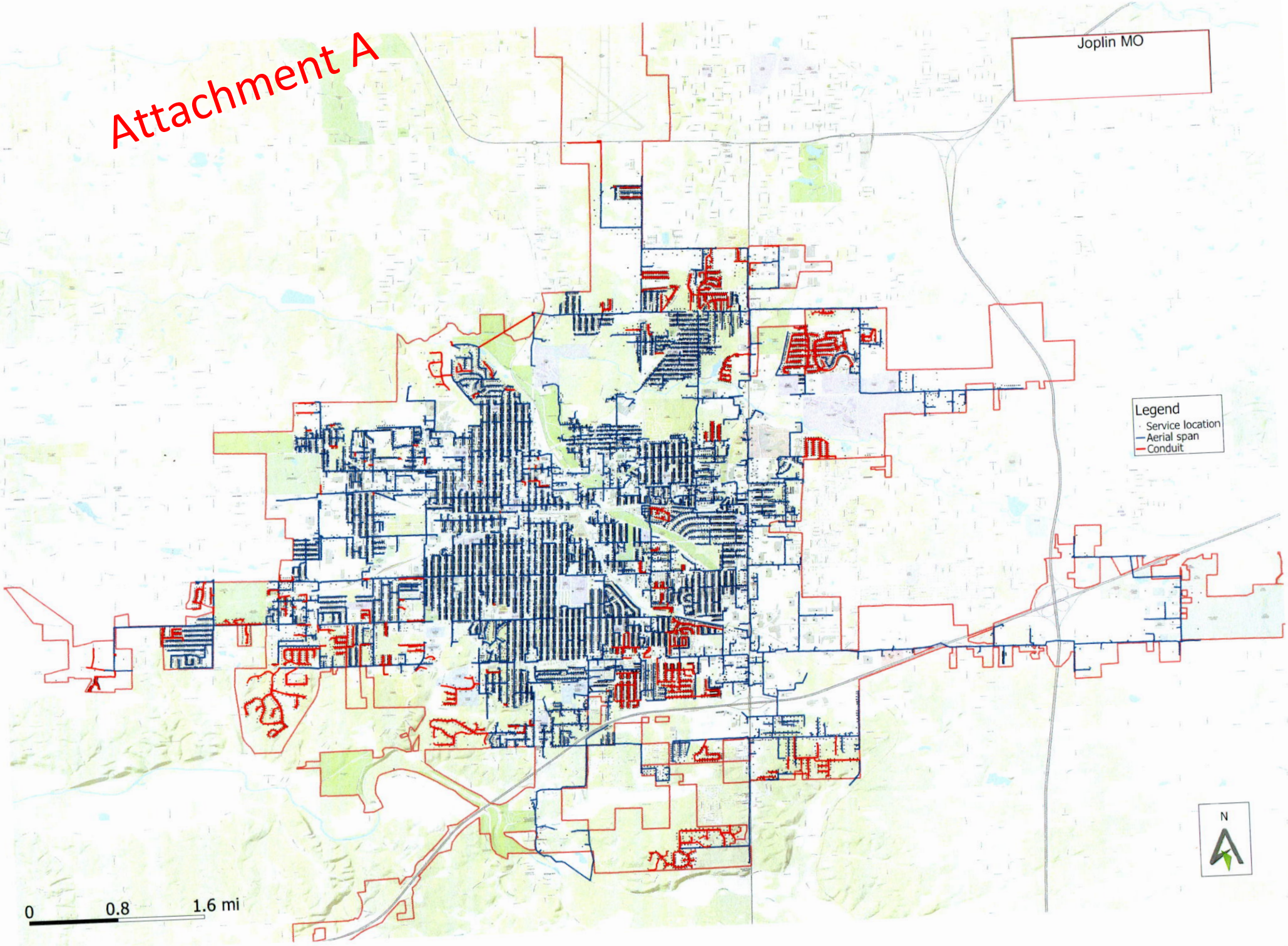
Bradley A. Moline

**CITY OF JOPLIN, MISSOURI**

By: _____

Nicholas Edwards
City Manager

Attachment A



Attachment B

| Joplin MO Attachment B - Construction Schedule | | |
|---|---|---|
| Event | Expected Completion Date | Requirements |
| Logistical Pre-Planning | Upon Award/Q1 2024 | |
| State and Local Agreements Executed | Q2 2024 (expected) | Including any required agreements required by local utilities. |
| Preliminary Design | Q2 2024 | |
| Permitting Approved | Q2 2024 | Dates are dependant upon underground and aerial construction permits being approved by the city and local utilities. |
| Communication of Construction | Q2 2024 | |
| Materials On-Site | Q2 2024 | |
| Construction Starts | Q2 2024 | Date dependant upon approval of an adequate number of permits to allow for efficient construct of the initial PON and transport routes. |
| Pre-Sale Marketing Ramp-Up | Q1 2025 | |
| Customer Operations Ready for Launch | Q1 2025 | |
| Fiber Hut(s) Commissioned | Q1 2025 | |
| Retail Sales Begin | Q1 2025 | |
| Initial Customer Drops Complete | Q1 2025 | |
| Network Testing | Q1 2025 | |
| Go Live to First Customers | Q1 2025 | 180 days after start of construction. |
| Fully Constructed | Q3 2026 | |
| Project Close Out | Q3 2026 | |

Attachment C



**Coronavirus State and Local Fiscal Recovery Funds: Treasury's 2022 Final Rule and 2023 IFR**

Treasury's 2022 final rule and 2023 IFR detail recipients' compliance responsibilities and provides additional information on eligible and restricted uses of SLFRF award funds and reporting requirements.

1. **Eligible and Restricted Uses of SLFRF Funds.** As described in the SLFRF statute and summarized above, there are seven eligible uses of SLFRF award funds. As a recipient of an award under the SLFRF program, your organization is responsible for complying with requirements for the use of funds. In addition to determining a given project's eligibility, recipients are also responsible for determining subrecipient's or beneficiaries' eligibility, and must monitor subrecipients' use of SLFRF award funds.

   To help recipients build a greater understanding of eligible uses, Treasury's 2022 final rule and 2023 IFR establish a framework for determining whether a specific project would be eligible under the SLFRF program, including some helpful definitions. For example, Treasury's 2022 final rule and 2023 IFR establish:
   - A framework for determining whether a project responds to the COVID-19 public health emergency or its negative economic impacts;
   - Definitions of "eligible employers," "essential work," "eligible workers," and "premium pay" for cases where premium pay is an eligible use;
   - The option to select between a standard amount of revenue loss or complete a full revenue loss calculation of revenue lost due to the COVID-19 public health emergency;
   - A framework for necessary water and sewer infrastructure projects that aligns eligible uses with projects that are eligible under the Environmental Protection Agency's Drinking Water and Clean Water State Revolving Funds along with certain additional projects, including a wider set of lead remediation and stormwater infrastructure projects and aid for residential wells;
   - A framework for necessary broadband projects that allows for projects that are designed to provide service of sufficient speeds to eligible areas, as well as an affordability requirement for providers that provide service to households;
   - A framework for determining how to provide emergency relief from a natural disaster;
   - Three pathways for using SLFRF funds for Surface Transportation projects along with the associated statutory requirements; and
   - A list of eligible Title I projects by reference to the activities that are eligible under the Community Development Block Program, along with the associated statutory requirements.

   Treasury's 2022 final rule also provides more information on important restrictions on use of SLFRF award funds, including that recipients other than Tribal governments may not deposit SLFRF funds into a pension fund; and recipients that are States or territories may not use SLFRF funds to offset a reduction in net tax revenue resulting from the recipient's change in law, regulation, or administrative interpretation. In addition, recipients may not use SLFRF funds directly to service debt, satisfy a judgment or settlement, or contribute to a "rainy day" fund. Recipients should refer to Treasury's 2022 final rule for more information on these restrictions and to the 2023 IFR for how these restrictions apply to the eligible uses added by the Consolidated Appropriations Act, 2023.

   Treasury's 2022 final rule outlines that funds available under the "revenue loss" eligible use category (sections 602(c)(1)(C) and 603(c)(1)(C) of the Social Security Act) generally may be used to meet the non-federal cost-share or matching requirements of other federal programs. However, the 2022 final rule notes that SLFRF funds may not be used as the non-federal share for purposes of a state's Medicaid and CHIP programs because the Office of Management and Budget ("OMB") has approved a waiver as requested by the Centers for Medicare & Medicaid Services pursuant to 2 CFR 200.102 of the Uniform Guidance and related regulations. If a recipient seeks to use SLFRF funds to satisfy match or cost-share requirements for a federal grant program, it should first confirm with the relevant awarding agency that no waiver has been granted for that program, that no other circumstances enumerated under 2 CFR 200.306(b) would limit the use of SLFRF funds to meet the match or cost-share requirement, and that there is no other statutory

or regulatory impediment to using the SLFRF funds for the match or cost-share requirement. Treasury's 2023 IFR outlines that under the Surface Transportation projects eligible use category, recipients may use SLFRF funds to satisfy non-federal cost share requirements for certain programs under Pathway Three. In addition, under the Title I projects eligible use category, recipients may use SLFRF funds to satisfy the non-federal share requirements of a federal financial assistance program in support of activities that would be eligible under the CDBG and ICDBG programs.

SLFRF funds beyond those that are available under the circumstances described above may not be used to meet the non-federal match or cost-share requirements of other federal programs, other than as specifically provided for by statute. For example, the Infrastructure Investment and Jobs Act provides that SLFRF funds may be used to meet the non-federal match requirements of authorized Bureau of Reclamation projects and certain broadband deployment projects.

Treasury's 2023 IFR describes the additional statutory restrictions that apply to the Surface Transportation projects and Title I projects eligible use categories. First, the total amount of SLFRF funds that a recipient may use for Surface Transportation projects and Title I projects, taken together, cannot exceed the greater of $10 million and 30% of a recipient's SLFRF allocation. Second, recipients using SLFRF funds for Surface Transportation projects and Title I projects must supplement, and not supplant, other federal, state, territorial, Tribal, and local government funds (as applicable) otherwise available for such uses. For the Surface Transportation projects eligible use category, recipients using funds for projects eligible for Urbanized Formula Grants, Fixed Guideway Capital Investment Grants, Formula Grants for Rural Areas, State of Good Repair Grants, or Grants for Buses and Bus Facilities may not use SLFRF funds for operating expenses of these projects.

2. **Eligible Costs Timeframe.** For eligible use categories described in the 2022 final rule, your organization, as a recipient of an SLFRF award, may use SLFRF funds to cover eligible costs that your organization incurred during the period that begins on March 3, 2021 and ends on December 31, 2024, as long as the award funds for the obligations incurred by December 31, 2024 are expended by December 31, 2026. Costs incurred for projects by the recipient State, territorial, local, or Tribal government prior to March 3, 2021 are not eligible, as provided for in Treasury's 2022 final rule.

   For eligible use categories described in the 2023 IFR, recipients may use SLFRF funds for the three new eligible uses for costs incurred beginning December 29, 2022. Consistent with the existing eligible uses, recipients must obligate SLFRF funds for the new eligible uses by December 31, 2024. Recipients must expend SLFRF funds obligated to provide emergency relief from natural disasters by December 31, 2026. Recipients must expend SLFRF funds obligated for Surface Transportation projects and Title I projects by September 30, 2026. Costs for projects described in the 2023 IFR that are incurred by the recipient State, territorial, local, or Tribal government prior to December 29, 2022 are not eligible under these three eligible use categories.

   Recipients may, in certain circumstances, use SLFRF award funds for the eligible use categories described in Treasury's 2022 final rule for costs incurred prior to March 3, 2021. Specifically,

   **a.** Public Health/Negative Economic Impacts: Recipients may use SLFRF award funds to provide assistance to households, small businesses, and nonprofits to respond to the public health emergency or negative economic impacts of the pandemic – such as rent, mortgage, or utility assistance – for costs incurred by the beneficiary (e.g., a household) prior to March 3, 2021, provided that the recipient State, territorial, local or Tribal government did not incur the cost of providing such assistance prior to March 3, 2021.

   **b.** Premium Pay: Recipients may provide premium pay retrospectively for work performed at any time during the COVID-19 public health emergency. Such premium pay must be "in addition to" wages and remuneration already received and the obligation to provide such premium pay must not have been incurred by the recipient prior to March 3, 2021.

   **c.** Revenue Loss: Recipients have broad discretion to use funds for the provision of government services to the extent of reduction in revenue. While calculation of lost revenue is based on the

recipient's revenue in the last full fiscal year prior to the COVID-19 public health emergency, use of funds for government services must be forward looking for costs incurred by the recipient after March 3, 2021.

**d.** Investments in Water, Sewer, and Broadband: Recipients may use SLFRF award funds to make necessary investments in water, sewer, and broadband infrastructure. Recipients may use SLFRF award funds to cover costs incurred for eligible projects planned or started prior to March 3, 2021, provided that the project costs covered by the SLFRF award funds were incurred by the recipient after March 3, 2021.

Any funds not obligated or expended for eligible uses by the timelines above must be returned to Treasury, including any unobligated or unexpended funds that have been provided to subrecipients and contractors as part of the award closeout process pursuant to 2 C.F.R. 200.344(d). For the purposes of determining expenditure eligibility, "incurred" means the recipient has incurred an obligation, which has the same meaning given to "financial obligation" in 2 CFR 200.1. See 31 CFR 35.5(b).

3. **Reporting.** Generally, recipients must submit one initial Interim Report, quarterly or annual Project and Expenditure reports which include subaward reporting, and in some cases annual Recovery Plan reports. Treasury's 2022 final rule, 2023 IFR, and Part 2 of this guidance provide more detail around SLFRF reporting requirements.

4. **Expenditure Categories**. Treasury's 2022 final rule provides greater flexibility and simplicity for recipients to fight the pandemic and support families and businesses struggling with its impacts, maintain vital services amid revenue shortfalls, and build a strong, resilient, and equitable recovery. As such, recipients report on a broader set of eligible uses and associated Expenditure Categories ("EC"), which began with the April 2022 Project and Expenditure Report. Appendix 1 includes the new ECs, as well as a reference to previous ECs used for reporting under the 2021 IFR.

The 2023 IFR implements the amendments to the SLFRF program made by the Consolidated Appropriations Act, 2023, which provides additional flexibility for recipients to use SLFRF funds to respond to natural disasters, build critical infrastructure, and support community development. The additional ECs associated with the 2023 IFR began with the October 2023 Project and Expenditure Report. These ECs also may be found in Appendix 1.

## Assistance Listing

The Assistance Listing for the Coronavirus State and Local Fiscal Recovery Funds (SLFRF) was published May 28, 2021 on SAM.gov under Assistance Listing Number ("ALN"), formerly known as CFDA Number, **21.027**.

The assistance listing includes helpful information including program purpose, statutory authority, eligibility requirements, and compliance requirements for recipients. The ALN is the unique 5-digit number assigned to identify a federal assistance listing, and can be used to search for federal assistance program information, including funding opportunities, spending on USASpending.gov, or audit results through the Federal Audit Clearinghouse.

To expedite payments and meet statutory timelines Treasury issued initial payments under an existing ALN, 21.019, assigned to the CRF. If you have already received funds or captured the initial number in your records, please update your systems and reporting to reflect the new ALN 21.027 for the SLFRF program. **Recipients must use ALN 21.027 for all financial accounting, subawards, and associated program reporting requirements for the SLFRF awards.**

## Uniform Administrative Requirements

The SLFRF awards are generally subject to the requirements set forth in the Uniform Guidance. In all instances, your organization should review the Uniform Guidance requirements applicable to your organization's use of SLFRF funds, and SLFRF-funded projects. Additional details about applicability of certain provisions of the Uniform Guidance may be found in:

- SLFRF 2022 final rule;
- SLFRF Assistance Listing;
- SLFRF 2022 Final Rule FAQs, including FAQ 4.9, 10.1, and Section 13; and
- SLFRF 2023 IFR.

The following sections provide a general summary of your organization's compliance responsibilities under applicable statutes and regulations, including the Uniform Guidance, as described in the most recent compliance supplement issued by OMB. Note that the descriptions below are only general summaries and all recipients and subrecipients are advised to carefully review the Uniform Guidance requirements and any additional regulatory and statutory requirements applicable to the program.

1. **Allowable Activities.** Each recipient should review program requirements, including Treasury's 2022 final rule, 2023 IFR, and the recipient's Award Terms and Conditions, to determine and record eligible uses of SLFRF funds. Per 2 CFR 200.303, your organization must develop and implement effective internal controls to ensure that funding decisions under the SLFRF award constitute eligible uses of funds, and document determinations.

2. **Allowable Costs/Cost Principles.** As outlined in the Uniform Guidance at 2 CFR Part 200, Subpart E regarding Cost Principles, allowable costs are based on the premise that a recipient is responsible for the effective administration of Federal awards, application of sound management practices, and administration of Federal funds in a manner consistent with the program objectives and terms and conditions of the award. Recipients must implement robust internal controls and effective monitoring to ensure compliance with the Cost Principles, which are important for building trust and accountability. Please note that as outlined in 2022 Final Rule FAQ 13.15, only a subset of the Uniform Guidance requirements at 2 CFR Part 200 Subpart E (Cost Principles) applies to recipients' use of funds in the revenue loss eligible use category.

   SLFRF funds may be, but are not required to be, used along with other funding sources for a given project. Recipients should note that SLFRF funds available under the "revenue loss" eligible use category generally may be used to meet the non-federal cost-share or matching requirements of other federal programs. If a recipient seeks to use SLFRF funds to satisfy match or cost-share requirements for a federal grant program, the recipient should first confirm with the relevant awarding agency that no waiver has been granted for that program, that no other circumstances enumerated under 2 CFR 200.306(b) would limit the use of SLFRF funds to meet the match or cost-share requirement, and that there is no other statutory or regulatory impediment to using the SLFRF funds for the match or cost-share requirement. For instance, recipients should note that SLFRF funds may not be used as the non-federal share for purposes of a state's Medicaid and CHIP programs because the OMB has approved a waiver from this provision as requested by the Centers for Medicare & Medicaid Services pursuant to 2 CFR 200.102 of the Uniform Guidance and related regulations.

   Treasury's 2023 IFR outlines that under the Surface Transportation projects eligible use category, recipients may use SLFRF funds to satisfy non-federal cost share requirements for certain programs under Pathway Three. In addition, under the Title I projects eligible use category, recipients may use SLFRF funds to satisfy the non-federal share requirements of a federal financial assistance program in support of activities that would be eligible under the CDBG and ICDBG programs.

   SLFRF funds beyond those that are available under the circumstances described above may not be used to meet the non-federal match or cost-share requirements of other federal programs, other than as specifically provided for by statute. As an example, the Infrastructure Investment and Jobs Act provides

that SLFRF funds may be used to meet the non-federal match requirements of authorized Bureau of Reclamation projects and certain broadband deployment projects. Recipients should consult the 2022 final rule for further details if they seek to utilize SLFRF funds as a match for these projects.

Treasury's 2022 final rule, 2023 IFR, program guidance, and the Uniform Guidance outline the types of costs that are allowable, including certain audit costs. For example, per 2 CFR 200.425, a reasonably proportionate share of the costs of audits required by the Single Audit Act Amendments of 1996 are allowable; however, costs for audits that were not performed in accordance with 2 CFR Part 200, Subpart F and the Compliance Supplement are not allowable. Please see 2 CFR Part 200, Subpart E regarding the Cost Principles for more information.

**a.** Administrative costs*:* Recipients may use funds for administering the SLFRF program, including costs of consultants to support effective management and oversight, including consultation for ensuring compliance with legal, regulatory, and other requirements.[2] Further, costs must be reasonable and allocable as outlined in 2 CFR 200.404 and 2 CFR 200.405. Pursuant to the SLFRF Award Terms and Conditions, recipients are permitted to charge both direct and indirect costs to their SLFRF award as administrative costs as long as they are accorded consistent treatment per 2 CFR 200.403. Direct costs are those that are identified specifically as costs of implementing the SLFRF program objectives, such as contract support, materials, and supplies for a project. Indirect costs are general overhead costs of an organization where a portion of such costs are allocable to the SLFRF award such as the cost of facilities or administrative functions like a director's office.[34] Each category of cost should be treated consistently in like circumstances as direct or indirect, and recipients may not charge the same administrative costs to both direct and indirect cost categories, or to other programs. If a recipient has a current Negotiated Indirect Costs Rate Agreement ("NICRA") established with a Federal cognizant agency responsible for reviewing, negotiating, and approving cost allocation plans or indirect cost proposals, then the recipient may use its current NICRA. Alternatively, if the recipient does not have a NICRA, the recipient may elect to use the de minimis rate of 10 percent of the modified total direct costs pursuant to 2 CFR 200.414(f).

**b.** Salaries and Expenses*:* In general, certain employees' wages, salaries, and covered benefits are an eligible use of SLFRF award funds. Please see Treasury's 2022 final rule for details.

**3. Cash Management.** SLFRF payments made to recipients are not subject to the requirements of the Cash Management Improvement Act and Treasury's implementing regulations at 31 CFR Part 205 or 2 CFR 200.305(b)(8)-(9).

As such, recipients can place funds in interest-bearing accounts, do not need to remit interest to Treasury, and are not limited to using that interest for eligible uses under the SLFRF award.

**4. Eligibility and Unique Entity Identifier Requirements.** Under the SLFRF program, recipients are responsible for ensuring that award funds are used for eligible purposes. Accordingly, recipients must develop and implement policies and procedures, and retain records, to determine and monitor implementation of criteria for determining the eligibility of beneficiaries and/or subrecipients. Your organization, and if applicable, the subrecipient(s) administering a program on behalf of your organization, will need to develop and maintain procedures for obtaining information evidencing a given beneficiary's, subrecipient's, or contractor's eligibility, including ensuring subrecipients and contractors are in good standing in accordance with 2 CFR 200.214 and 2 CFR Part 200, Appendix II, paragraph (H).
Further, recipients and subrecipients are required to obtain a valid Unique Entity Identifier (UEI), which is assigned by SAM.gov. Pursuant to the award term regarding 2 CFR Part 25, Appendix A, which is incorporated by reference in the SLFRF Financial Assistance Agreement, recipients are required to maintain current information in SAM.gov for the duration of the period of performance of the SLFRF award. A recipient may not make a subaward to a subrecipient unless that subrecipient has obtained and provided to the recipient a UEI. Subrecipients are not required to complete full SAM.gov registration to obtain a UEI. A UEI is not required with respect to beneficiaries and contractors. Implementing risk-based

due diligence for eligibility determinations is a best practice to augment your organization's existing controls.

5. **Property Management.** Any purchase of real or personal property with SLFRF funds must be consistent with the Uniform Guidance at 2 CFR Part 200, Subpart D, unless stated otherwise by Treasury. For example, as outlined in 2022 Final Rule FAQ 13.15, only a subset of the Uniform Guidance requirements at 2 CFR Part 200 Subpart D (Post Federal Award Requirements) applies to recipients' use of funds in the revenue loss eligible use category. Furthermore, as outlined in 2022 Final Rule FAQ 13.16, Treasury has clarified the use and disposition requirements for real and personal property, supplies, and equipment purchased with SLFRF funds.

6. **Matching, Level of Effort, Earmarking.** There are no matching, level of effort, or earmarking compliance responsibilities associated with the SLFRF award. See Section C.1 (Eligible and Restricted Uses of SLFRF Funds) for a discussion of restrictions on use of SLFRF funds. Please see 2. Allowable Costs/Cost Principles above for information on the use of SLFRF funds for non- Federal match or cost-sharing requirements in other Federal programs.

7. **Period of Performance.** Your organization should also develop and implement internal controls related to activities occurring outside the period of performance. For eligible uses under the 2022 final rule, all funds remain subject to statutory and regulatory requirements that they must be used for costs incurred by the recipient during the period that begins on March 3, 2021, and ends on December 31, 2024, and that award funds for the financial obligations incurred by December 31, 2024 must be expended by December 31, 2026. For eligible uses under the 2023 IFR, recipients may use SLFRF funds for costs incurred beginning December 29, 2022. Consistent with the existing eligible uses, recipients must obligate SLFRF funds for the new eligible uses by December 31, 2024. Recipients must expend SLFRF funds obligated to provide emergency relief from natural disasters by December 31, 2026. Recipients must expend SLFRF funds obligated for Surface Transportation projects and Title I projects by September 30, 2026. Any funds not expended must be returned to Treasury as part of the award closeout process pursuant to 2 C.F.R. 200.344(d).

8. **Procurement, Suspension & Debarment.** Recipients are responsible for ensuring that any procurement using SLFRF funds, or payments under procurement contracts using such funds, are consistent with the procurement standards set forth in the Uniform Guidance at 2 CFR 200.317 through 2 CFR 200.327, unless stated otherwise by Treasury. As outlined in 2022 Final Rule FAQ 13.15, only a subset of the Uniform Guidance requirements at 2 CFR Part 200 Subpart D (Post Federal Award Requirements) applies to recipients' use of funds in the revenue loss eligible use category. The procurement standards set forth in the Uniform Guidance at 2 CRF 200.317 through 2 CRF 200.327 are not included in 2022 Final Rule FAQ 13.15's list of applicable Subpart D requirements that apply to recipients' use of funds in the revenue loss eligible use category.

---

[2] Recipients also may use SLFRF funds directly for administrative costs to improve the design and execution of programs responding to the COVID-19 pandemic and to administer or improve the efficacy of programs addressing the public health emergency or its negative economic impacts. 31 CFR 35.6(b)(3)(ii)(E)(3).

[3] 2 CFR 200.413 Direct Costs.

[4] 2 CFR 200.414 Indirect Costs.

The Uniform Guidance establishes in 2 CFR 200.319 that all procurement transactions for property or services must be conducted in a manner providing full and open competition, consistent with standards outlined in 2 CFR 200.320, which allows for non-competitive procurements only in certain circumstances. Recipients must have and use documented procurement procedures that are consistent with the standards outlined in 2 CFR 200.317 through 2 CFR 200.320. In addition, the Uniform Guidance at 2 CFR 200.214, 2 CFR Part 180, and Treasury's implementing regulations at 31 CFR Part 19, prohibit recipients from entering into contracts with suspended or debarred parties. The procurement standards outlined in the Uniform Guidance require an infrastructure for competitive bidding and contractor oversight, including maintaining written standards of conduct. Your organization must ensure adherence to all applicable local, State, and federal procurement laws and regulations.

9. **Program Income.** Generally, program income includes, but is not limited to, income from fees for services performed, the use or rental of real or personal property acquired under Federal awards, and principal and interest on loans made with Federal award funds. Program income does not include interest earned on advances of Federal funds, rebates, credits, discounts, or interest on rebates, credits, or discounts. Recipients of SLFRF funds should calculate, document, and record the organization's program income. Additional controls that your organization should implement include written policies that explicitly identify appropriate allocation methods, accounting standards and principles, compliance monitoring checks for program income calculations, and records.

   The Uniform Guidance outlines the requirements that pertain to program income at 2 CFR 200.307. Treasury has clarified in its 2022 Final Rule FAQs that recipients may add program income to the Federal award. Any program income generated from SLFRF funds must be used for the purposes and under the conditions of the Federal award. Further, 2022 Final Rule FAQ 4.9 provides additional information about program income requirements applicable to certain eligible uses, and 2022 Final Rule FAQ 13.15 clarifies that only a subset of the Uniform Guidance requirements at 2 CFR 200 Subpart D (Post Federal Award Requirements) applies to recipients' use of funds in the revenue loss eligible use category. The list of applicable Subpart D requirements in 2022 Final Rule FAQ 13.15 does not include the program income requirements in 2 CFR 200.307.

10. **Reporting.** All recipients of federal funds must complete financial, performance, and compliance reporting as required and outlined in Part 2 of this guidance. Expenditures may be reported on a cash or accrual basis, as long as the methodology is disclosed and consistently applied. Reporting must be consistent with the definition of expenditures pursuant to 2 CFR 200.1. Your organization should appropriately maintain accounting records for compiling and reporting accurate, compliant financial data, in accordance with appropriate accounting standards and principles.

    In addition, where appropriate, your organization needs to establish controls to ensure completion and timely submission of all mandatory performance and/or compliance reporting. See Part 2 of this guidance for a full overview of recipient reporting responsibilities.

    Consolidated jurisdictions or other types of jurisdictions that received multiple SLFRF allocations (e.g., a county and city with a consolidated government) are only required to file once per reporting period, and such reports will cover the total SLFRF allocations received by the jurisdiction. This includes non-entitlement units of local government ("NEUs") and/or units of general local government located within counties that are not units of general local government. In addition, the total SLFRF allocations across all sources for a given jurisdiction will be used to identify that jurisdiction's Reporting Tier.

11. **Subrecipient Monitoring.** SLFRF recipients that are pass-through entities as described under 2 CFR 200.1 are required to manage and monitor their subrecipients to ensure compliance with requirements of the SLFRF award pursuant to 2 CFR 200.332 regarding requirements for pass- through entities.

    First, your organization must clearly identify to the subrecipient: (1) that the award is a subaward of SLFRF funds; (2) any and all compliance requirements for use of SLFRF funds; and (3) any and all reporting

requirements for expenditures of SLFRF funds.

Next, your organization will need to evaluate each subrecipient's risk of noncompliance based on a set of common factors. These risk assessments may include factors such as prior experience in managing Federal funds, previous audits, personnel, and policies or procedures for award execution and oversight. Ongoing monitoring of any given subrecipient should reflect its assessed risk and include monitoring, identification of deficiencies, and follow-up to ensure appropriate remediation.

Accordingly, your organization should develop written policies and procedures for subrecipient monitoring and risk assessment and maintain records of all award agreements identifying or otherwise documenting subrecipients' compliance obligations.

Recipients should note that NEUs are not subrecipients under the SLFRF program. They are SLFRF recipients that report directly to Treasury.

Recipients should also note that subrecipients do not include individuals and organizations that received SLFRF funds as end users. Such individuals and organizations are beneficiaries and not subject to audit pursuant to the Single Audit Act and 2 C.F.R. Part 200, Subpart F.

Many recipients may choose to provide a subaward or contract to other entities to provide services to other end users. For example, a recipient may provide a subaward to a nonprofit to provide homeless services to individuals experiencing homelessness. In this case, the subaward to a nonprofit is based on the services that the recipient intends to provide (assistance to households experiencing homelessness), and the nonprofit is serving as the subrecipient, providing services on behalf of the recipient. Subrecipients are subject to an audit pursuant to the Single Audit Act and 2 CFR part 200, subpart F regarding audit requirements, whereas contractors are not subject to an audit pursuant to the Single Audit Act and 2 CFR part 200, subpart F regarding audit requirements.

Please note that as outlined in 2022 Final Rule FAQ 13.14, recipients' use of funds in the revenue loss eligible use category does not give rise to subrecipient relationships. As a result, subaward reporting is not required for projects in the revenue loss eligible use category.

**12. Special Tests and Provisions.** From time-to-time, Treasury may issue subregulatory guidance as well as frequently asked questions.

Across each of the compliance requirements above, Treasury has described some best practices for development of internal controls in **Table 1** below, with an example of each best practice.

Table 1: Internal controls best practices

| Best Practice | Description | Example |
|---|---|---|
| **Written policies and procedures** | Formal documentation of recipient policies and procedures | Documented procedure for determining worker eligibility for premium pay |
| **Written standards of conduct** | Formal statement of mission, values, principles, and professional standards | Documented code of conduct / ethics for subcontractors |
| **Risk-based due diligence** | Pre-payment validations conducted according to an assessed level of risk | Enhanced eligibility review of subrecipient with imperfect performance history |
| **Risk-based compliance monitoring** | Ongoing validations conducted according to an assessed level of risk | Higher degree of monitoring for projects that have a higher risk of fraud, given program characteristics |

| Best Practice | Description | Example |
|---|---|---|
| **Record maintenance and retention** | Creation and storage of financial and non-financial records. | Storage of all subrecipient payment information. |

## B. Award Terms and Conditions

The Award Terms and Conditions of the SLFRF financial assistance agreement sets forth the compliance obligations for recipients pursuant to the SLFRF statute, the Uniform Guidance, Treasury's 2022 final rule, 2023 IFR, and applicable federal laws and regulations. Recipients should ensure they remain in compliance with all Award Terms and Conditions. These obligations include the following items in addition to those described above:

1. **SAM.gov Requirements.** All eligible recipients are required to have an active registration with the System for Award Management ("SAM") (https://www.sam.gov) pursuant to 2 CFR Part 25. To ensure timely receipt of funding, Treasury has stated that NEUs who have not previously registered with SAM.gov may do so after receipt of the award, but before the submission of mandatory reporting.[5]

2. **Recordkeeping Requirements.** Generally, your organization must maintain records and financial documents for five years after all funds have been expended or returned to Treasury, as outlined in paragraph 4.c. of the Award Terms and Conditions. Treasury may request transfer of records of long-term value at the end of such period. Wherever practicable, such records should be collected, transmitted, and stored in open and machine-readable formats.

   Your organization must agree to provide or make available such records to Treasury upon request, and to the Government Accountability Office ("GAO"), Treasury's Office of Inspector General ("OIG"), and their authorized representative in order to conduct audits or other investigations.

3. **Single Audit Requirements.** Recipients and subrecipients that expend more than $750,000 in Federal awards during their fiscal year will be subject to an audit under the Single Audit Act and its implementing regulation at 2 CFR Part 200, Subpart F regarding audit requirements.[6] Note that the Compliance Supplement provides information on the existing, important compliance requirements that the federal government expects to be considered as a part of such audit. For example, the SLFRF Compliance Supplement describes an alternative to the Single Audit for eligible recipients. Recipients should consult the Compliance Supplement for more information about the alternative compliance examination engagement. The Compliance Supplement is routinely updated, and is made available in the Federal Register and on OMB's website: https://www.whitehouse.gov/omb/office-federal-financial-management/ Recipients and subrecipients should consult the Federal Audit Clearinghouse to see examples of Single Audit submissions.

4. **Civil Rights Compliance**. Recipients of Federal financial assistance from the Treasury are required to meet legal requirements relating to nondiscrimination and nondiscriminatory use of Federal funds. Those requirements include ensuring that entities receiving Federal financial assistance from the Treasury do not deny benefits or services, or otherwise discriminate on the basis of race, color, national origin (including limited English proficiency), disability, age, or sex (including sexual orientation and gender identity), in accordance with the following authorities: Title VI of the Civil Rights Act of 1964 (Title VI) Public Law 88-352, 42 U.S.C. 2000d-1 et seq., and the Department's implementing regulations, 31 CFR part 22; Section 504 of the Rehabilitation

   Act of 1973 (Section 504), Public Law 93-112, as amended by Public Law 93-516, 29 U.S.C. 794; Title IX of the Education Amendments of 1972 (Title IX), 20 U.S.C. 1681 et seq., and the Department's implementing regulations, 31 CFR part 28; Age Discrimination Act of 1975, Public Law 94-135, 42 U.S.C. 6101 et seq., and the Department implementing regulations at 31 CFR part 23.

   In order to carry out its enforcement responsibilities under Title VI of the Civil Rights Act, Treasury will

collect and review information from recipients to ascertain their compliance with the applicable requirements before and after providing financial assistance. Treasury's implementing regulations, 31 CFR part 22, and the Department of Justice (DOJ) regulations, Coordination of Non-discrimination in Federally Assisted Programs, 28 CFR part 42, provide for the collection of data and information from recipients (see 28 CFR 42.406). Treasury may request that non-tribal recipients submit data for post-award compliance reviews, including information such as a narrative describing their Title VI compliance status. As explained in Treasury FAQ 12.1, the award terms and conditions for Treasury's pandemic recovery programs, including the SLFRF program, do not impose antidiscrimination requirements on Tribal governments beyond what would otherwise apply under federal law.

[5] See flexibility provided in https://www.whitehouse.gov/wp-content/uploads/2021/03/M_21_20.pdf.

[6] For-profit entities that receive SLFRF subawards are not subject to Single Audit requirements. However, they are subject to other audits as deemed necessary by authorized governmental entities, including Treasury and Treasury's OIG.

Attachment D

# Disaster Recovery Matrix/Overview (Complete Loss)

| Scenario 1 (Complete Loss) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Infrastructure** | **Risk Example** | **Phase 0** | **Phase 1** | **Phase 2** | **Phase 3** | **Phase 4** | **Phase 5** | **Limitations/Gaps** |
| | | **0 to 4 Hours** | **0 to 24 Hours** | **24 to 72 Hours** | **72 Hours to 1 Week** | **72 Hours to 2 Weeks** | **72 Hours to 4 Weeks** | |
| | | | | | | | | |
| **Critical Infrastructure** | - Destruction of HUB (Tornado, Fire, Flood) | - Assessment:<br>- What is salvageable?<br>- What needs to be replaced?<br>- ***Resources: CI Team*** | - Execute Generator strategy<br>- Tent site construction<br>- Raze existing structure<br>- Portable HVAC Installation<br>- Order Thermobond replacement structure<br>- ***Resources: CI Team, Termobond, Caterpillar, Interstate*** | - Replacement of tent with framed structure (as required)<br>- ***Resources: CI Team, Field Operations*** | - Installation of new Thermobond structure<br>- Installation of permanent HVAC<br>- Installation of permanent power source<br>- ***Resources: CI Team, Thermobound, Field Operations*** | | | |
| **IPTV/Video** | - Destruction of HUB/Headend | - Assessment:<br>- What is salvageable?<br>- What needs to be replaced?<br>- ***Resources: Video Op's*** | - Order required hardware<br>- ***Resources: Video Op's*** | - Initiate new hardware installation<br>- ***Dependencies: Network Engineering (Connectivity), CI***<br>- ***Resources: Video Op's*** | - Finalize installation of hardware<br>- ***Resources: Video Op's, Contractors*** | | | - No Tangerine sparing for complete hardware replacement ***($250K)***<br>- Lack of satellite content backup<br>- ***Impact: 75 Channels***<br>- ***Cost: $240K***<br>***($40K in 2021 budget)*** |
| **cCFS Network/Voice** | - Destruction of Data Center | - Assessment:<br>- What is salvageable?<br>- What needs to be replaced?<br>- ***Resources: Voice Op's*** | - Order required hardware<br>- **Resources: Voice Op's** | - Initiate new hardware installation<br>- Voice VRF Firewall required for MVS client access (management access to Voice network environment)<br>- ***Dependencies: Network Engineering (Connectivity), CI***<br>- ***Resources: Voice Op's*** | - Repair/install server & SAN hardware<br>- Establish new VMware environment<br>- ***Resources: Voice Op's, Nelnet*** | - Critical server restoration<br>- cCFS Network- Cisco ASA Firewall Voice<br>- ***Resources: Voice Op's, Nelnet*** | - Recovery of specific services based on network resources.<br>- ***Resources: Voice Op's, Nelnet*** | - No immediate replacement for Metaswitch UMG (CH6010)<br>- No immediate replacement for ADTRAN Multiplexer hardware<br>- Risk Low due to redundancy<br>- ***Impact: Potential Capacity Issues (Voice Degradation)***<br>- ***Cost: $40K*** |
| **Data Center** | - Destruction of Data Center | - Assessment<br>- What is salvageable?<br>- What needs to be replaced?<br>- What apps/services can run on surviving infrastructure?<br>- What apps require manual tasks to complete failover?<br>- **Resources: Network/Sys Engineering, Nelnet** | - Order required hardware<br>- **Resources: Network/Sys Engineering, Nelnet** | - Initiate new hardware installation<br>- **Dependencies: Network Engineering (Connectivity), CI**<br>- **Resources: Network/Sys Engineering, Nelnet** | - Repair/install server & SAN hardware<br>- Establish new VMware environment<br>- ***Resources: Network/Sys Engineering, Nelnet*** | - Critical server restoration<br>- Site specific UCS Central VM<br>- Site specific vCenter<br>- Backup storage (images, configuration files, etc)<br>- Local bastion host<br>- Nelnet CommVault (off-site backups)<br>- ***Resources: Sys Engineering, Nelnet*** | - Recovery of specific services based on network resources<br>- ***Resources: Sys Engineering, Nelnet*** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Production Network (Core)** | - Destruction of backbone site (tornado, flood, fire) | - Assessment<br>- What is salvageable?<br>- What needs to be replaced?<br>- What transport/peering vendors need to be engaged?<br>- Confirm traffic failover to other transit/peers/CDN's<br>- Monitor failover capacity<br>- Manually move individual customers to alternate datacenter if possible<br>- ***Resources: Network/Sys Engineering*** | - Order required hardware<br>- Fiber restoration to cage/rack by Allo OSP and/or datacenter staff<br>- ***Resources: Network/Sys Engineering, Nelnet*** | - Repair/Install new routing/switching hardware<br>- Using shelf spares, install minimally viable hardware in modified configuration to restore backbone, peering & market diversity<br>- ***Dependencies: CI***<br>- ***Resources: Network Engineering*** | - Establish external connectivity<br>- Work with transport providers to restore all backbone circuits<br>- Work with peers to bring core peering/DIA back online<br>- Work with Allo OSP/transport providers to restore diversity to impacted markets<br>- ***Resources: Network/Sys Engineering, Transport Carriers, Peers, CDN Providers*** | - Remove temporary router/switch configuration & replace with original state<br>- Install/turn up CDN appliances, working with content provider to commission<br>- ***Resources: Network/Sys Engineering, Peers, CDN Providers*** | | - Lack of Hardware sparing (PDU's, Routers, Servers, Line Cards)<br>- ***Impact: Nearly 100% Internet Degradation/Loss***<br>- ***Cost: $1.5M*** |
| **Production Network (Aggregation)** | - Destruction of HUB site (tornado, flood, fire) | - Assessment<br>- What is salvageable?<br>- What new hardware is required (routers, switches, optics, access gear, fiber jumpers, fuse panels, etc)?<br>- ***Resources: Network Engineering*** | - Order required hardware<br>- Fiber restoration to cage/rack by Allo OSP and/or datacenter staff<br>- ***Resources: Network/Sys Engineering, Nelnet*** | - Repair/Install new routing/switching hardware<br>- Using shelf spares, install minimally viable hardware in modified configuration to restore backbone, peering & market diversity<br>- Backups for all gear stored on Rancid, CMS or FTP server<br>- ***Dependencies: CI***<br>- ***Resources: Network Engineering*** | - Work with Allo OSP to restore all backbone fiber to HUB<br>- Work with Allo OSP Team to restore distribution and feeder routers.<br>- ***Resources: Network Engineering, Allo OSP*** | - Remove temporary router/switch configuration & replace with original state<br>- Install/turn up CDN appliances, working with content provider to commission<br>- ***Resource: Network Engineering*** | | - Lack of hardware sparing (Calix, etc.)<br>- ***Impact: Nearly 100% Internet Degradation/Loss***<br>- ***Cost: $1.1M*** |

| Critical Infrastructure | | | | | | |
|---|---|---|---|---|---|---|
| **Infrastructure** | **Element** | **Sparing** | **Location** | **Replacement ETA** | **Contact** | **Notes** |
| Structure | Hardened (12’ X 30’) | Yes | Elk Point, SD | 24-72 Hours | Thermobond | Michael Kastning (SE- Thermobond): 712-251-2125 |
| Structure | Remote Cabinets | Yes | Lincoln | 4-8 Hours | CI Team | Warehouse Spare |
| Racks/Equipment | Racks | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Fiber Guide | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Runway | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | PDU’s | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Rectifier System | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Batteries | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | HVAC Controller | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Vaonet | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Fiber Frame Components | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Jumpers | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Breakers & Fuse Panels | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Copper Wire | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Racks/Equipment | Connector Lugs | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |

| | | | | | | |
|---|---|---|---|---|---|---|
| Racks/Equipment | Door Card Reader | Yes | Lincoln, SB, NP | 8-12 Hours | CI Team | Warehouse Spares |
| Power | Generator- Large | Yes | Varies | 4-8 Hours | Interstate/Cat | Interstate: 800-222-6060<br>Caterpillar: 800-736-8228 |
| Power | Generator- Temp | Yes | Lincoln, SB, NP | 4-8 Hours | CI Team | Warehouse |

| IPTV/Video | | | | | | |
|---|---|---|---|---|---|---|
| **Infrastructure** | **Element** | **Sparing** | **Location** | **Replacement ETA** | **Contact** | **Notes** |
| IPTV Headend | IRD's | Yes | SB | 4-8 Hours | Video Op's Team | Same location, +1 sparing |
| IPTV Headend | Encoders | Yes | SB | 4-8 Hours | Video Op's Team | Same location, +1 sparing |
| IPTV Headend | Servers | Yes | SB | 4-8 Hours | Video Op's Team | Same location, +1 sparing |
| IPTV Headend | Hard Drives | Yes | SB | 4-8 Hours | Video Op's Team | Same location, +1 sparing |
| IPTV Headend | Satellite Dishes | No | | | | Planning (3) 4.5m dishes in NP |
| Mediaroom Headend | Servers | Yes | NP | 4-8 Hours | Video Op's Team | Same location, +1 sparing |
| Mediaroom Headend | Tangerine | Yes | NP | 4-8 Hours | Video Op's Team | Tangerine spare parts box |
| Remote | OTA Receivers | Yes | SB | 4-8 Hours | Video Op's Team | Shelf spare in SB, backup channel source in most markets |
| Remote | EAS | Yes | SB | 4-8 Hours | Video Op's Team | Shelf spare in SB, backup channel source in most markets |

| cCFS Network/Voice (Hardware) | | | | | | |
|---|---|---|---|---|---|---|
| **Server Type** | **Element** | **Sparing** | **Location** | **Replacement ETA** | **Contact** | **Notes** |
| Perimeta SBC | Dell R640 | Yes | BLV | 4-8 Hours | Voice Op's/Nelnet | Lincoln Warehouse |
| Cisco Firewall | Cisco ASA | Yes | BLV | 4-8 Hours | Voice Op's/Nelnet | Lincoln Warehouse |
| Cisco Firewall | Cisco ASA | Yes | BLV | 4-8 Hours | Voice Op's/Nelnet | Lincoln Warehouse |
| Cisco Firewall | Cisco ASA | Yes | DEN | 4-8 Hours | Nelnet | Voice VRF Firewall managed by Nelnet |
| Perimeta SBC | Dell R640 | Yes | LNK | 4-8 Hours | Video Op's | Lincoln Warehouse |
| Cisco Firewall | Cisco ASA | Yes | LNK | 4-8 Hours | Voice Op's | Lincoln Warehouse |
| Metaswitch UMG | CH6010 | No | LNK | 24-72 Hours | Voice Op's/Metaswitch | Spares via Metaswitch |
| ADTRAN Multiplexer | Opti | No | ALN | 24-72 Hours | Voice Op's/ADTRAN | Spares via ADTRAN |
| Metaswitch UMG | CH6010 | No | SCB | 24-72 Hours | Voice Op's/Metaswitch | Spares via Metaswitch |
| ADTRAN Multiplexer | Opti | No | SCB | 24-72 Hours | Voice Op's/ADTRAN | Spares via ADTRAN |

| cCFS Network/Voice (VM/Server) | | | | | | |
|---|---|---|---|---|---|---|
| **Server Type** | **Element** | **#** | **Location** | **Replacement ETA** | **Contact** | **Notes** |
| Metasphere EAS | VM | 1 | DEN | 4-8 Hours | Voice Op's/Nelnet | 12 CPU, 24GB Mem, 1000GB Disk |
| Metaswitch AMGC | VM | 2 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 12 CPU, 48GB Mem, 200GB Disk |
| Metaswitch CFS | VM | 2 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 12 CPU, 48GB Mem, 200GB Disk |

| | | | | | | |
|---|---|---|---|---|---|---|
| Metaswitch DCM | VM | 4 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 1 CPU, 1 GB Mem, 10GB Disk |
| Metaswitch MRS | VM | 6 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 8 CPU, 8GB Mem, 100GB Disk |
| Metaswitch N-Series | VM | 1 | DEN | 4-8 Hours | Voice Op's/Nelnet | 4 CPU, 8GB Mem, 100GB Disk |
| Metaswitch OBS | VM | 4 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 8 CPU, 16GB Mem, 100GB Disk |
| Metaswitch RPAS | VM | 4 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 4 CPU, 4GB Mem, 100GB Disk |
| Metaswitch SAS | VM | 1 | DEN | 4-8 Hours | Voice Op's/Nelnet | 12 CPU, 24GB Mem, 4TB Disk |
| Metaview Director | VM | 2 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 4 CPU, 8GB Mem, 100GB Disk |
| Metaview MVS | VM | 2 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 12 CPU, 24GB Mem, 300GB Disk |
| OrecX Voice Recorder | VM | 1 | BLV | 4-8 Hours | Voice Op's/Nelnet | 4 CPU, 8GB Mem, 250GB Disk |
| Perimeta SBC | VM | 2 | BLV, DEN | 4-8 Hours | Voice Op's/Nelnet | 8 CPU, 16GB Mem, 40GB Disk, PCI |

# *Critical Infrastructure*

## ALLO CO/Headend Building and Cabinet Disaster Recovery Plan (3/8/2021)

- **Sparing/Availability**

  Structure

  Thermobond retains a 12'x30' structure in stock for use by ALLO in event of an emergency total loss situation. The structure is bare but would be outfitted and shipped within 24 hours from Elk Point South Dakota. Initiating this process would be the responsibility of Critical Infrastructure and would begin with the approval by the Director of OSP Engineering and notification to Thermobond of the emergency, Michael Kastning – Sales Engineering team – 712-251-2125.

  Other Remote Cabinets

  ALLO has a spare cabinet in stock in Lincoln Nebraska to respond to a total loss cabinet situation. Contact Critical Infrastructure team member to initiate the process. Expected restoration time <8 hours.

  Critical Infrastructure Racks and Equipment

  ALLO has the following spare items stored at our Lincoln, Scottsbluff, or North Platte Warehouses:

  - Racks
  - Fiber guide
  - Runway
  - PDUs
  - Rectifier System
  - Batteries
  - HVAC Controller
  - Vaonet
  - Fiber Frame components
  - Jumpers
  - Breakers and fuse panels
  - Copper wire
  - Connector lugs
  - Door Card reader

  Contact a Critical Infrastructure team member to initiate the process.

Generators

ALLO has contracts in place with both Interstate and Catapiller to respond 24/7 with large trailer generators to restore power at any CO/headend site in the ALLO network within 4 hours.

ALLO maintains smaller portable generators at the Lincoln, Scottsbluff, and North Platte warehouses to restore cabinet sites.

Interstate call out 1-800-222-6060
Catapillar call out 1-800-RENT CAT 1-800-736-8228

**o Plan**

Scenario 1 – Total Loss – Structure Unusable (Tornado / Fire / Etc)

Disaster Assessment – 4 hours

- What is salvageable?
- What needs to be ordered for Critical Infrastructure structure and equipment?

Phase 1 – Infrastructure Replacement (Plan will come from CI Team) – first 24 hours

- Determine power availability at the site – execute generator sparing strategy as required by the situation.
- Tent site and start splicing on fiber to extend to new frame
- Raze existing site if unusable
- The existing pad/foundation may be used to install racks, power, and restore service if possible using portable HVAC inside of the tent and spare equipment/racks – execute sparing strategy as required by the situation.
- Order replacement structure from Thermobond for immediate shipping and overnight any other needed items.

Phase 2 – Consider replacing tent with framed/plywood structure – as required

Phase 3 – Install new Thermobond structure and new equipment for a permanent replacement. – as required

Initate by contracting Critical Infrastructure team member.

Scenario 2 – Partial Loss – Structure Usable (Flood, Vandelism, Accident, Weather, Etc)

Disaster Assessment – 2 hours

- What is salvageable?

- What needs to be ordered for Critical Infrastructure structure repair and equipment?

Phase 1 – Structure repair plan (Plan will come from CI Team) – next 2 hours

- Determine power availability at the site – execute generator sparing strategy as required by the situation.
- Use portable HVAC units for cooling if existing units are unrepairable.
- If needed tent site until repairs to the structure can be completed.
- If needed start splicing to restore fiber.
- Install needed repair items and equipment into the existing structure.
- Order any needed replacement structure components from Thermobond for immediate shipping and overnight any other needed items.

Phase 2 – Complete permanent repairs as components are received.

Initate by contracting Critical Infrastructure team member.

<u>Scenario 3 – Single Item Loss (Generator, HVAC, Rectifier, Etc)</u>

Phase 1 – Replace or repair any items damaged with a spare. Order replacement spare as soon as possible. – 4 hours

- Resources required (internal, 3rd party)

Scenario 1: Critical Infrastructure Team, Construction, IPTV Team, Crane contractor, and other contractors as needed.

Scenario 2: Critical Infrastructure Team, Construction, IPTV Team, and other contractors as needed.

Scenario 3: Critical Infrastructure Team and other contractors as needed.

- Testing of plan

Scenario 1: Test using tabletop exercises and review lessons learned from Ashland flooding of CO cabinet site.

Scenario 2: Test using tabletop exercises.

Scenario 3: Test using tabletop exercises and review lessons learned from past component failures.

- Communication Plan

  Internal Communications:

  During a service impacting event we will follow the standard outage communication protocol. (Need to insert a link to the current outage process here)

  Vendor Communications:

  Directly with vendors as required by Critical Infrastructure and Supply teams.

  FCC Communications: https://www.fcc.gov/network-outage-reporting-system-nors

  For Scenario 1, 2, and 3, outages of more than 30 minutes, the outage must be reported to the FCC by Corporate Communications.

  External Communications:

  During a service impacting event we will follow the standard outage communication protocol. (Need to insert a link to the current outage process here)

  No information should be released to news outlets without prior approval of Corporate Communications.

The Critical Infrastructure Team, to contact us call or email:

- Supervisor James Dobesh 402-417-4014 (james.dobesh@allofiber.com)
- Mark Znamenacek 402-646-8639 (mark.znamernacek@allofiber.com)
- Jason Davis 308-220-8047 (jason.davis@allofiber.com)
- Escalations to Al Schroeder 402-430-5958 (al.schroeder@allofiber.com)

## Market Emergency HVAC callout numbers

| Market | Vendor | Phone Number |
|---|---|---|
| North Platte | Knobel Refrigeration | 308-532-2665 |
| Lincoln and Ashland | Capitol Heating and Air | 402-483-6080 |
| Ogallala | Correl Refrigeration | 308-284-6715 |
| Norfolk | Volkman Plumbing and Heating | 402-371-0316 |
| Bridgeport | Polar Express | 308-221-4368 |
| Scottsbluff and Gering | Polar Express | 308-221-4368 |
| Scottsbluff HE | Data Power | 402-592-7860 |
| Alliance | Jacks Refrigeration | 308-646-3827 |
| Fort Morgan | Bob Staley Plumbing and Heating | 970-867-5262 |
| Breckenridge | Breckenridge Mechanical | 970-453-1950 |
| Imperial | Troxells Heaing and Appliance | 308-882-4497 |
| Hastings | Rutts Heating and Air Conditioning | 402-463-4853 |

# *IPTV/Video*

ALLO IPTV Disaster Recovery Plan (1/18/2021)

## o Sparing/Availability

IPTV Headend (Scottsbluff)

**Hardware (IRDs, Encoders, Servers, Hard Drives)**
Current solution is a +1 sparing, meaning either there is a spare online ready to be swapped to or a shelf spare. The shelf spares are currently stored at the same physical location as the production system. Inventory is done every 6 months.

**Satellite Dishes**
No sparing for the 3.8-meter dishes in Scottsbluff. Plan to erect 3 x 4.5-meter dishes in North Platte for some redundancy.

Mediaroom Headend (North Platte)

**Hardware (Mediaroom Servers / Tangerine)**
Current solution is a +1 sparing, meaning there is a spare online ready to be swapped to. Tangerine has a spare parts box for extra hard drives, and other parts which is in the HUT.

Other Remote HUTs/COs

**Hardware (Over the air receivers, EAS (Emergency Alert Systems)**
Current solution is a shelf spare located at the Scottsbluff office. Most all sites have a backup channel source so having an in-market spare is not required.

## o Plan

Scenario 1 – Total Loss (Tornado / Fire / Etc)

**Disaster Assessment –**

- **What is salvageable?**
- **What needs to be ordered for equipment?**

**Phase 1 – Infrastructure Replacement (Plan will come from CI Team)**
**Phase 2 – Connectivity (Plan will come from Network)**
**Phase 3 – Install of new IPTV equipment and restore IPTV Service**
**Utilize contractors as needed to speed recovery.**

Scenario 2 – Partial Loss (Flood, Malware, Ransomware, Etc)

**Disaster Assessment –**

- **What is salvageable?**
- **What needs to be ordered for equipment?**

**Phase 1 – Infrastructure Replacement (Plan will come from CI Team)**
**Phase 2 – Connectivity (Plan will come from Network)**
**Phase 3 – Replace or repair any items damaged, utilize contractors to speed recovery.**

Scenario 3 – Single Item Loss (Server, Hard Drive, Receiver, Etc)

**Phase 1 – Replace or repair any items damaged with hot spare or shelf spare.**
**Order replacement spare as soon as possible.**

- Resources required (internal, 3rd party)

Scenario 1: Critical Infrastructure Team, Network Engineering Team, IPTV Team, Tangerine Global, Outside contractors as needed.
Scenario 2: Critical Infrastructure Team, Network Engineering Team, IPTV Team, Tangerine Global, Outside contractors as needed.
Scenario 3: IPTV Team, Tangerine Global

- Testing of plan

Scenario 1: Since there is not full redundancy this plan cannot be tested.

Scenario 2: Since there is not full redundancy this plan cannot be tested.

Scenario 3: This event commonly occurs and is tested at least once a year. Making sure we have an accurate sparing plan is the most crucial. Inventory every 6 month is required.

- Risk Assessment. Incremental planning depending on market.

Scottsbluff: **Satellite and Local Channels Affected for all markets (1/4 of all channels).** EAS affected for all markets.
Gering: No impact to other markets. No IPTV assets located in this market.
Bridgeport: No impact to other markets. No IPTV assets located in this market.
Alliance: No impact to other markets. No IPTV assets located in this market.

Ogallala: No impact to other markets. No IPTV assets located in this market.
North Platte: EAS for Ogallala, Imperial, and North Platte.
**IPTV down for all markets (Tangerine Servers located here).**
Imperial: No impact to other markets. No IPTV assets located in this market.
Hastings: Backup over the air receivers located here. EAS covering Hastings market.
Lincoln: Depending on site affected – we have Lincoln locals from over the air from NCC building and the NetNet building. EAS is located at the NCC building which serves Lincoln and Omaha.
Ashland Lakes: No impact to other markets. No IPTV assets located in this market.
Omaha: No impact to other markets. No IPTV assets located in this market.
Fort Morgan: Three over the air channels with no backups will be affected for Fort Morgan Only. EAS for Fort Morgan will be affected.
Breckenridge: EAS for Breckenridge will be affected.
Fremont: No impact to other markets. No IPTV assets located in this market.
Norfolk: EAS for Norfolk will be affected.

- Communication Plan

Internal Communications:

During a service impacting event we will follow the standard outage communication protocol. (Need to insert link to current outage process here)

Vendor Communications:

Tangerine – Need support ticket opened.
Other vendors as needed.

FCC Communications: https://www.fcc.gov/network-outage-reporting-system-nors

For Scenario 1 and 2 outages more than 30 minutes long issues must be reported to the FCC.

Other Communications: If this affects other downstream customers individual communications will be needed.

PinPoint (Shared Mediaroom)
Great Plains (Shared Locals)
USA Communications (Shared Locals)
Hamilton Communications (Shared Locals)
Cozad Communications (Shared Locals)

# *cCFS Network/Voice*

# ALLO Voice Network Disaster Recovery Plan

## Overview & Scope

This DR plan details the affect and recovery of various failures in the ALLO Voice network.

Table of Contents:


- Assumptions and audience
- Voice network services overview
    - Voices Telephony Services and priorities
    - Voice network summary
    - Sites utilized
    - Voice server network element list
- Site specific Disaster Plan
    - Services affected for site loss as well as individual server loss
    - Manual tasks needed to restore services
    - Critical servers required to restore all priority services
- Appendix A – Individual Server Sparing and Availability
- Appendix B – Individual Server Restoral Process
- Appendix C – FCC/PUC/PSC Communications (details needed)
- Appendix D – Outstanding questions/action items


## Assumptions and audience

- This document is intended for an audience with general understanding of TDM/VoIP telephony voice networks and services as well as the Metaswitch clustered CFS topology.
- Infrastructure, external connectivity, VMware host environment are prerequisite to restoring the Voice Network. This is covered in the *Data Center Disaster Recovery Plan*.
- Metaswitch Customer Support services can be used for assistance with the restoral of Metaswitch network elements and may be required for the cleanup of CFS subscriber rehoming.
- The TDM trunking interconnection via ADTRAN OPTI 6100 Multiplexers is located in many sites in the ALLO network. Disaster Recovery for OPTI Multiplexers are included in the *Network Transport Disaster Recovery Plan*.
- Safety and security of associates takes priority over recovery activities.
- In an extensive disaster event staff & equipment resources may be insufficient, which in turn will prolong recovery activities.
- Depending on the severity of the incident, customers and other ALLO teams may be required to modify their operations to accommodate differences in applications/services until a full recovery has been completed. This may include manual processing for an extended period of time.
- Outstanding action items to improve inefficiencies are listed in appendix D.

## Voice network services overview

### *Voice telephony services*

The Allo Voice network is made up of hardware and software components that provides telephony services including but not limited to the following:

- Basic telephone services
    - Residential analog and VoIP telephone – Priority 1
    - Business analog and VoIP telephone – Priority 1
    - Enterprise PBX analog and VoIP interconnection – Priority 1
    - Max UC Desktop and Mobile softphone client – Priority 1
    - Caller ID – Priority 2
    - Robocall blocking – Priority 4
    - Call Forwarding – Priority 2
    - Three-Way Calling – Priority 3
    - Fax/Data – Priority 2
    - DTMF Interworking – Priority 2
- Advanced Business Features
    - Auto Attendant – Priority 1
    - Advanced Call Distribution – Priority 2
    - Multi Line Hunt Group – Priority 2
    - Line State Monitoring – Priority 2
    - Call Park/Pickup – Priority 2
- Enhanced Application Features
    - Voicemail – Priority 3
    - Commportal Web Services – Priority 3
    - Orecx call media recording – Priority 4
    - Large Conference – Priority 3
    - Music on Hold – Priority 4
    - SIP-TLS and SRTP encryption – Priority 1
- Call routing services
    - Inbound Local and LD call services – Priority 1
    - Outbound Local interconnection Services – Priority 1
    - Outbound LD Services – Priority 1
    - Toll Free 800 inbound and outbound services – Priority 1
    - 911 Emergency access – Priority 1
- Management Services
    - Billing services – Priority 2
    - Provisioning services – Priority 2
    - Alarm monitoring services – Priority 3
    - SAS call logging services – Priority 3

Priorities:

- Priority 1: Critical priority voice service – These services are the first to be restored

- Priority 2: High priority voice service – These services are critical as well but are second priority
- Priority 3: Medium priority voice service – These services have lesser priority than the critical services
- Priority 4: Low priority voice service – these services take least precedence when restoring services

  Note: Certain customers take priority over others (E.G. the State of NE, cities and healthcare providers) as determined by Customer Operations.

### *Allo Voice networks*

The Allo Voice network includes the original Legacy network and the new geo-redundant Clustered CFS (cCFS) network. We are in the process of migrating all customers off of the Legacy network and onto the cCFS network. Approximately 95% of the Allo Voice customer base resides on the cCFS network. The following lists include sites that house the Voice Network server elements and does not include any additional VoIP and TDM transport locations which should be included in the Allo Network/Transport plans.

- Legacy network
  - site-redundant VM based components in Bellevue NE - BLV11
  - hardware based components in Scottsbluff NE – SCB01 and SCB11

- cCFS network
  - site and geo-redundant VM based components in Bellevue NE – BLV11
  - site and geo-redundant VM based components in Denver CO – DEN11
  - hardware based components in Lincoln NE – LNK01
  - hardware based components in Scottsbluff NE – SCB01
  - State of NE hardware based components in Bellevue NE – BLV11
  - State of NE hardware based components in Lincoln NE – LNK23

### *Allo Voice network sites and servers*

- BLV11 – TierPoint data center, Bellevue, NE. - Primary data center for Voice services
  - cCFS Voice Server Network Elements
    - Metaswitch Allo-BLV-cCFS-MVS – primary Metaview Element Monitoring System
    - Metaswitch Allo-BLV-cCFS-AMGC – primary Access Media Gateway Controller
    - Metaswitch Allo-BLV-CFS – primary Call Feature Server
    - Metaswitch Perimeta Allo-ISC2 – primary Session Border Controller
    - Metaswitch Allo-BLV-MVD – primary MetaView Director
    - Metaswitch Allo-BLV-SAS – primary Service Assurance Server
    - Metaswitch Allo-BLV-MRS1,MRS2,MRS3 – Media Resource Servers
    - Metaswitch Allo-BLV-OBS1,OBS2 – Object Backup Store Servers
    - Metaswitch Allo-BLV-RPAS1,RPAS2 – Representative App Servers

        - Metaswitch Allo-BLV-DCM1,DCM2 – Distributed Capacity Manager Servers
        - Metaswitch Perimeta SON-BLV-ISC1 – secondary State of NE Session Border Controller
        - OrecX Allo-BLV-ORK1 – Call Recording server
        - Cisco BLV11-FW06 – primary Voice-VRF firewall for EAS web services and IPSec VPN
        - Cisco SON-OMA-FW – secondary State of NE firewall for EAS web services
    - Legacy Voice Network Elements
        - Metaswitch Allo-BLV-MVS – Metaview Element Monitoring System
        - Metaswitch Allo-CA1 – Call Feature Server
        - Metaswitch Allo-Omaha-MVD – MetaView Director
        - Metaswitch Allo-BLV11-SAS – Service Assurance Server
        - Metaswitch Allo-DCM1,DCM2 – Distributed Capacity Manager Servers
        - Metaswitch Allo-BLV11-SAS – Service Assurance Server
        - Metaswitch Omaha-EAS – Enhanced Application Server
        - Metaswitch Omaha-N-Series – N-Series Application Server
        - Cisco BLV11-FW01 – Legacy firewall for EAS web services

- DEN11 – 910 Telecom, Denver, CO. - Primary data center for cCFS network Voice services
    - cCFS Voice Network Elements
        - Metaswitch Allo-DEN-cCFS-MVS – primary Metaview Element Monitoring System
        - Metaswitch Allo-DEN-cCFS-AMGC – primary Access Media Gateway Controller
        - Metaswitch Allo-DEN-CFS – primary Call Feature Server
        - Metaswitch Perimeta Allo-ISC3 – primary Session Border Controller
        - Metaswitch Allo-DEN-MVD – primary MetaView Director
        - Metaswitch Allo-DEN-SAS – primary Service Assurance Server
        - Metaswitch Allo-DEN-MRS1,MRS2,MRS3 – Media Resource Servers
        - Metaswitch Allo-DEN-OBS1,OBS2 – Object Backup Store Servers
        - Metaswitch Allo-DEN-RPAS1,RPAS2 – Representative App Servers
        - Metaswitch Allo-DEN-DCM1,DCM2 – Distributed Capacity Manager Servers
        - Metaswitch Allo-DEN-EAS – Enhanced Application Server
        - Metaswitch Allo-DEN-NSR – N-Series Application Server
        - Cisco BLV11-FW06 – primary Voice-VRF firewall for EAS web services and IPSec VPN

- SCB01 – Scottsbluff headend/hub – cCFS TDM Voice services, Legacy Voice Services
    - cCFS Voice Network Elements
        - Metaswitch  Allo-SCB-UMG – primary Universal Media Gateway
    - Legacy Voice Network Elements
        - Metaswitch Perimeta Allo-SCB-ISC1 – Session Border Controller
        - Metaswitch ALNCNE-UMG – primary Universal Media Gateway

- SCB11 – Scottsbluff Lumen CO – TDM Voice Services
    - Legacy Voice Network Elements
        - Metaswitch SCTSNE-UMG – primary Universal Media Gateway

- LNK01 – Lincoln #1 hub – cCFS TDM Voice Services
    - cCFS Voice Network Elements
        - Allo-LCN-UMG – primary Universal Media Gateway

- LNK23 – State of NE data center – State of NE VoIP Voice services
    - cCFS Voice Network Elements
        - Metaswitch Perimeta SON-LCN-ISC1 – primary State of NE Session Border Controller
        - Cisco SON-LCN-FW – primary State of NE firewall for EAS web services

### *Server Sparing/Availability*

Spares are not currently stocked for most components. Replacements provided by vendor support agreements. Also, SAN arrays and Metaswitch voice core are remotely monitored by their respective vendors. See Appendix A for list of voice network elements with redundancy, availability and sparing details.

# BLV11 Site Plan

## Scenario 1 – Total Loss of Bellevue BLV11 site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

### *Service impact*

cCFS network subscribers:

- Basic telephone services
  - Residential analog – outage until manual switchover
  - Residential VoIP telephone – impact limited to associated services
  - Business analog – outage until manual intervention
  - Business VoIP telephone – impact limited to associated services
  - Enterprise PBX analog interconnection – outage until manual intervention
  - Enterprise PBX VoIP interconnection – limited outage requires manual intervention
  - Max UC Desktop and Mobile softphone client – impact limited to associated services
  - Caller ID – no impact
  - Robocall blocking – no impact
  - Call Forwarding – no impact
  - Three-Way Calling – no impact
  - Fax/Data – no impact
  - DTMF Interworking – no impact
- Advanced Business Features
  - Auto Attendant – no impact
  - Advanced Call Distribution – no impact
  - Multi Line Hunt Group – no impact
  - Line State Monitoring – no impact
  - Call Park/Pickup – no impact
- Enhanced Application Features
  - Voicemail – no impact
  - Commportal Web Services – no impact
  - Orecx call media recording – Total service outage
  - Large Conference – outage until Legacy Omaha-N-Series is restored
  - Music on Hold – no impact
  - SIP-TLS and SRTP encryption – no impact
- Call routing services
  - Inbound Local and LD call services – Partially affected, outage until manual intervention
  - Outbound Local interconnection Services – Calls will reroute to Denver SIP
  - Outbound LD Services – Calls will reroute to Denver SIP

        - Toll Free 800 inbound – Partially affected, outage until manual intervention
        - Toll Free outbound services – Calls will reroute to Denver SIP
        - 911 Emergency access – Calls will reroute to BW SIP 911
    - Management Services
        - Billing services – no impact
        - Provisioning services – must use Allo-DEN-cCFS-MVS for MVWeb or MVS client
        - Alarm monitoring services – must use Allo-DEN-cCFS-MVS
        - SAS call logging services – must use Allo-DEN-cCFS-SAS, partially impacted requires manual intervention

Legacy network subscribers:

    - All services – Outage until Legacy servers are brought back in service or subscribers are migrated to cCFS

Phase 0 – Execute or Confirm Service Failover

- What services can run on the surviving site?
    - cCFS Network
        - Most cCFS network services and features can run on the surviving sites.
        - All TDM services (SS7 and H.248) require manual AMGC switchover from Bellevue to Denver.
        - Dynamic subscribers will rehome to Denver site automatically.
        - H.248 and SIP devices hardcoded to Bellevue will need manual redirect to Denver.
        - Inbound SS7 ISUP trunk calls and outbound TollFree TCAP800 calls will require SS7 switchover to Allo-DEN-AMGC.
        - Outbound SS7 ISUP trunk calls will reroute to SIP overflow trunks until SS7 switchover to Allo-DEN-AMGC.
        - OrecX call recording service is simplex in Bellevue and will be out of service.
        - Large Conference currently uses Legacy Omaha-N-Series. Outage will be incurred until server is restored or service is manually migrated to cCFS Allo-DEN-NSR server.
        - Remote SSH management of Voice network will need to bypass the BLV-Voice-VRF-FW.
        - Denver Jump server can be used as SSH proxy.
        - There will be no Denver MVS Client access via VPN. Either Metaswitch support will need to be contacted, or someone must connect directly from the Voice-VRF network at one of our site locations.
        - MVWeb Provisioning and SAS Logging will have to be redirected to Denver site.
    - Legacy Network
        - The Legacy network will experience a full outage with loss of BLV11 site.

- What applications require manual tasks to complete failover?

- SSH access to Voice network elements will have to be accomplished via Denver Jump server or Metaswitch Customer Support assistance.
- TDM services (SS7 and H.248) require manual AMGC switchover from Bellevue to Denver.
- ISUP trunk calls (inbound/outbound) and outbound TollFree TCAP800 requires SS7 switchover to Allo-DEN-AMGC
  - Enable Syniverse SS7 A-Links on the Allo-DEN-AMGC
  - Ensure Calix H.248 profile points to DEN-AMGC as signaling gateway
- H.248 devices hardcoded to Bellevue will need manual redirect to Denver.
  - Ensure Calix OLT Profile includes Allo-DEN-AMGC as signaling server
- SIP devices hardcoded to Bellevue will need manual redirect to Denver.
  - Configure any SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Denver (Allo-DEN-CFS or Allo-DEN-ISC3 as needed).
  - Configure any State of NE SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Allo-DEN-CFS or SON-LCN-ISC1 as needed.
- MVWeb Provisioning and SAS Logging will have to be redirected to Denver site
  - Ensure all users use the Denver systems instead of Bellevue (Allo-DEN-cCFS-MVS and Allo-SAS-cCFS-MVS)
- Allo-DEN-MVS activations as management server for UMGs
  - Activate Allo-LCN-UMG and Allo-SCB-UMG on the Allo-DEN-cCFS-MVS
- Allo-DEN-SAS activation as SAS call logging server for Lincoln UMG
  - Point Allo-LCN-UMG to Allo-DEN-cCFS-SAS for logging
  - Point SoN-LCN-ISC1 to Allo-DEN-cCFS-SAS for logging
- N-Series Large Conference will be out of service until Legacy Omaha-N-Series is restored or service is manually migrated to Allo-DEN-NSR server
- Legacy network subscribers may need to be migrated to the cCFS on a priority basis.

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

- Voice-VRF Firewall BLV11-FW06 is required for MVS client access for management access  ssh access to Voice network environment

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

These Servers/VMs should be restored in order to recover all Priority 1 and Priority 2 services.

- cCFS Network
  - Cisco ASA Firewall Voice-VRF BLV11-FW06

- Legacy Network
  - Metaswitch DCM Allo-DCM1
  - Metaview MVS Allo-BLV-MVS1
  - Metaswitch CFS AlloCA1
  - Metaview Director MVD
  - Metasphere EAS Omaha-EAS
  - Cisco ASA Firewall Legacy BLV11-FW01

### *Phase 5 – Recover specific services*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

## Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *cCFS Network*

- Metaview Server Allo-BLV-cCFS-MVS
  Similar to Scenario 1 if server cannot be recovered in a timely manner. Allo-DEN-cCFS-MVS can take over MVWeb provisioning and network monitoring capabilities for all Eastern NE network elements.

- Metaswitch SAS Allo-BLV-cCFS-SAS
  Similar to Scenario 1 if server cannot be recovered in a timely manner Allo-DEN-cCFS-SAS can take over call logging functions for all Eastern NE network elements.

- Metaswitch AMGC Allo-BLV-AMGC
  No impact for loss of a single VM instance.
  Similar to Scenario 1 for loss of VM pair, Allo-DEN-AMGC will take over for Allo-BLV-AMGC

- Metaswitch CFS Allo-BLV-CFS
  No impact for loss of a single VM instance.
  Similar to Scenario 1 for loss of VM pair, Allo-DEN-CFS will take over for Allo-BLV-CFS

- Metaswitch MRS Allo-BLV-MRS1, Allo-BLV-MRS2, Allo-BLV-MRS3

No loss of service for any outage of these servers. The other MRS servers including in Denver will take over for any server that is lost.

- Metaview Director Allo-BLV-MVD
  No impact for loss of a single VM instance.
  Loss of server pair will result in Bellevue CFS subscribers rehoming to Denver CFS.

- Metaswitch OBS Allo-BLV-OBS1, Allo-BLV-OBS2
  No loss of service for any outage of these servers. The other OBS servers including in Denver will take over for any server that is lost.

- Metaswitch RPAS Allo-BLV-RPAS1, Allo-BLV-RPAS2
  No loss of service for any outage of these servers. The other RPAS servers including in Denver will take over for any server that is lost.

- Metaswitch DCM Allo-BLV-DCM1,Allo-BLV-DCM2
  No loss of service for any outage of these servers. The other DCM servers including in Denver will take over for any server that is lost.
- Metaswitch Perimeta SBC Allo-BLV-ISC2
  No impact for loss of a single VM instance.
  Similar to Scenario 1 for loss of VM pair, Allo-DEN-ISC3 will take over for Allo-BLV-ISC2

- OrecX Call recording Server Allo-BLV-ORK1
  The lower priority OrecX call recording service will not function until the Allo-BLV-ORK1 server is brought back into service.

- Cisco ASA firewall BLV-Voice-VRF-FW
  No impact for loss of a single server.
  Similar to Scenario 1 for loss of server pair. DEN-Voice-VRF-FW will take over for BLV-Voice-VRF-FW for most services.
  Bellevue FW Syniverse SS7 A-Links will go out of service and Denver FW Syniverse SS7 A-Links will take over SS7 services.
  Default gateway static routes may need to be changed to point to DEN-Voice-VRF-FW instead of BLV-Voice-VRF-FW.
  VPN connectivity to Voice network including access to Denver MVS will be lost. Allo access would be from computer inside Voice-VRF or via Metaswitch support who has direct access via Metaswitch VPN through Denver firewall.

- Metaswitch Perimeta SBC SON-BLV-ISC1
  No impact for loss of a single Dell server.
  Similar to Scenario 1 for loss of Dell server pair, SON-LCN-ISC1 will take over for SON-BLV-ISC1.

- Cisco ASA firewall SON-OMA-FW
  No impact for loss of a single Cisco ASA server.

Similar to Scenario 1 for loss of Cisco ASA server pair, SON-LCN-FW will take over for SON-OMA-FW.

### *Legacy Network*

- Metaswitch DCM Allo-DCM1, Allo-DCM2
  No impact for loss of a single VM instance. Upon loss of both VM instances, no provisioning of additional licensed features is allowed.

- Metaview Server Allo-BLV-MVS1
  Similar to Scenario 1 if server cannot be recovered in a timely manner Metasview server Allo-DNV-MVS2 can take over provisioning and monitoring capabilities for the Legacy network

- Metaview Server Allo-DNV-MVS2
  No impact for loss of standby Metaview server Allo-DNV-MVS2

- Metaswitch CFS Allo-CA1
  No impact for loss of a single VM instance. Similar to Scenario 1 for loss of VM pair.

- Metaview Director Allo-Omaha-MVD-1
  No impact for loss of a single VM instance. Since Legacy network has a single CFS server and EAS server, and 95% of all remaining subscriber base connect to the network via PBX lines, very little impact will be experienced with loss of MVD pair.

- Metaswitch SAS Allo-BLV11-SAS
  Loss of service logging will take effect upon loss of Allo-BLV11-SAS. No impact to legacy subscriber services.

- Metaswitch N-Series OMAHA-N-Series
  Loss of N-Series conferencing service will take effect upon loss of Omaha-N-Series server. Any subscribers using Legacy N-series conference can be configured on cCFS N-Series and use the Conference service on the cCFS network.

- Metasphere EAS OMAHA-EAS
  Loss of Voicemail and Auto Attendant services will take effect upon loss of Omaha-EAS server. All Auto Attendants can be configured to route to default numbers. If server cannot be recovered in a timely manner, all affected subscribers should be migrated to the cCFS.

- Legacy FW
  No impact for loss of a single FW server. All EAS Commportal and N-Series Conference web services will be lost upon outage of Legacy FW server pair. Similar to Scenario 1 for loss of server pair.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan.  Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol.  *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# DEN11 Site Plan

## Scenario 1 – Total Loss of Denver BLV11 site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

### *Service impact*

cCFS network subscribers:

- Basic telephone services
  - Residential analog – impact limited to associated services
  - Residential VoIP telephone – impact limited to associated services
  - Business analog – impact limited to associated services
  - Business VoIP telephone – impact limited to associated services
  - Enterprise PBX analog interconnection – impact limited to associated services
  - Enterprise PBX VoIP interconnection – limited outage requires manual intervention
  - Max UC Desktop and Mobile softphone client – impact limited to associated services
  - Caller ID – no impact
  - Robocall blocking – no impact
  - Call Forwarding – no impact
  - Three-Way Calling – no impact
  - Fax/Data – no impact
  - DTMF Interworking – no impact
- Advanced Business Features
  - Auto Attendant – outage until Allo-DEN-EAS is restored
  - Advanced Call Distribution – outage until Allo-DEN-EAS is restored
  - Multi Line Hunt Group – no impact
  - Line State Monitoring – no impact
  - Call Park/Pickup – no impact
- Enhanced Application Features
  - Voicemail – outage until Allo-DEN-EAS is restored
  - Commportal Web Services – outage until Allo-DEN-EAS is restored
  - Orecx call media recording – no impact
  - Large Conference – no impact
  - Music on Hold – outage until Allo-DEN-NSR has been restored
  - SIP-TLS and SRTP encryption – no impact
- Call routing services
  - Inbound Local and LD call services – no impact
  - Outbound Local interconnection Services – no impact

        - Outbound LD Services – Calls will reroute to Bellevue SIP
        - Toll Free 800 inbound – no impact
        - Toll Free outbound services – no impact
        - 911 Emergency access – no impact
    - Management Services
        - Billing services – no impact
        - Provisioning services – must use Allo-BLV-cCFS-MVS for MVWeb or MVS client
        - Alarm monitoring services – must use Allo-BLV-cCFS-MVS
        - SAS call logging services – must use Allo-BLV-cCFS-SAS, partially impacted requires manual intervention

Legacy network subscribers:

- All services - impact similar to cCFS network

### *Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surviving site?
    - cCFS Network
        - Most cCFS network services and features can run on the surviving sites
        - All dynamic subscribers will rehome to Bellevue site automatically.
          H.248 and SIP devices hardcoded to Denver will need manual redirect to Bellevue.
        - MVWeb Provisioning and SAS Logging will have to be redirected to Bellevue site
- What applications require manual tasks to complete failover?
    - SIP devices hardcoded to Denver will need manual redirect to Bellevue.
        - Configure any SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Bellevue (Allo-BLV-CFS or Allo-BLV-ISC2 as needed).
        - Configure any State of NE SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Allo-BLV-CFS or SON-BLV-ISC1 as needed.
    - MVWeb Provisioning and SAS Logging will have to be redirected to Bellevue site
        - Ensure all users use the Bellevue systems instead of Denver (Allo-DEN-cCFS-MVS and Allo-DEN-cCFS-SAS)
    - Allo-DEN-MVS activations as management server for UMGs
        - Activate Allo-LCN-UMG and Allo-SCB-UMG on the Allo-DEN-cCFS-MVS
    - Allo-DEN-SAS activation as SAS call logging server for Lincoln UMG
        - Point Allo-LCN-UMG to Allo-DEN-cCFS-SAS for logging
        - Point SoN-LCN-ISC1 to Allo-DEN-cCFS-SAS for logging
    - Allo-DEN-EAS Voicemail, Auto-Attendant, Commportal and SIPPS services will be out of service.
    - Music On-Hold services will be out of service.
- What applications require manual tasks to complete failover?
    - SIP devices hardcoded to Denver will need manual redirect to Bellevue.
        - Configure any SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Denver (Allo-BLV-CFS or Allo-BLV-ISC3 as needed).

        - Configure any State of NE SIP end-user devices (e.g. ADTRAN 600) with simplex SIP signaling or proxy servers to point to Allo-BLV-CFS or SON-BLV-ISC1 as needed.
    - MVWeb Provisioning and SAS Logging will have to be redirected to Bellevue site
        - Ensure all users use the Bellevue systems instead of Denver (Allo-BLV-cCFS-MVS and Allo-BLV-cCFS-SAS)
    - Allo-BLV-cCFS-SAS activation as SAS call logging server for Scottsbluff UMG
        - Point Allo-SCB-UMG to Allo-BLV-cCFS-SAS for logging

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

These Servers/VMs should be restored in order to recover all Priority 1 and Priority 2 services.

- cCFS Network
    - Metasphere EAS Allo-DEN-EAS
    - Cisco ASA Firewall Voice-VRF DEN11-FW01

### *Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

## Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *cCFS Network*

- Metaview Server Allo-DEN-cCFS-MVS
  Similar to Scenario 1 if server cannot be recovered in a timely manner Allo-BLV-cCFS-MVS can take over MVWeb provisioning and network monitoring capabilities for all Eastern NE network elements.

- Metaswitch SAS Allo-DEN-cCFS-SAS
  Similar to Scenario 1 if server cannot be recovered in a timely manner Allo-BLV-cCFS-SAS can take over call logging functions for all Eastern NE network elements.

- Metaswitch AMGC Allo-DEN-AMGC
  No impact for loss of standby Allo-DEN-AMGC. Allo-BLV-AMGC will remain as primary AMGC server.

- Metaswitch CFS Allo-DEN-CFS
  No impact for loss of a single VM instance.
  Similar to Scenario 1 for loss of VM pair, Allo-BLV-CFS will take over for Allo-DEN-CFS.

- Metaswitch MRS Allo-DEN-MRS1, Allo-DEN-MRS2, Allo-DEN-MRS3
  No loss of service for any outage of these servers. The other MRS servers including in Bellevue will take over for any server that is lost.

- Metaview Director Allo-DEN-MVD
  No impact for loss of a single VM instance.
  Loss of server pair will result in Denver CFS subscribers relocating to Bellevue CFS.

- Metaswitch OBS Allo-DEN-OBS1, Allo-DEN-OBS2
  No loss of service for any outage of these servers. The other OBS servers including in Bellevue will take over for any server that is lost.

- Metaswitch RPAS Allo-DEN-RPAS1, Allo-DEN-RPAS2
  No loss of service for any outage of these servers. The other RPAS servers including in Bellevue will take over for any server that is lost.

- Metaswitch DCM Allo-DEN-DCM1,Allo-DEN-DCM2
  No loss of service for any outage of these servers. The other DCM servers including in Bellevue will take over for any server that is lost.

- Metasphere EAS SBC Allo-DEN-EAS
  Similar to Scenario 1 for loss of EAS VM.
  Full outage of Voicemail, Auto-Attendant, and SIPPS SIP provisioning services.

- Metaswitch N-Series Allo-DEN-NSR
  Similar to Scenario 1 for loss of N-Series VM.
  Full outage of Music On Hold services. Any conferencing should be pointed to Legacy Bellevue N-Series server.

- Metaswitch Perimeta SBC Allo-DEN-ISC3
  No impact for loss of a single VM instance.
  Similar to Scenario 1 for loss of VM pair, Allo-BLV-ISC2 will take over for Allo-DEN-ISC3.

- Cisco ASA firewall DEN-Voice-VRF-FW
  No impact for loss of a single server.
  Similar to Scenario 1 for loss of server pair, BLV-Voice-VRF-FW will take over for DEN-Voice-VRF-FW. Denver FW Syniverse SS7 A-Links will go out of service and Bellevue FW Syniverse SS7 A-Links will take over SS7 services.
  Default gateway static routes may need to be changed to point to BLV-Voice-VRF-FW instead of DEN-Voice-VRF-FW.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan. Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# LNK04 Site Plan

## Scenario 1 – Total Loss of Lincoln LNK04 site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

### *Service impact*

cCFS network subscribers:

- Basic telephone services
  - Residential analog – no impact
  - Residential VoIP telephone – no impact
  - Business analog – no impact
  - Business VoIP telephone – no impact
  - Enterprise PBX analog interconnection – no impact
  - Enterprise PBX VoIP interconnection – no impact
  - Max UC Desktop and Mobile softphone client – no impact
  - CallerID – no impact
  - Robocall blocking – no impact
  - Call Forwarding – no impact
  - Three-Way Calling – no impact
  - Fax/Data – no impact
  - DTMF Interworking – no impact
- Advanced Business Features
  - Auto Attendant – no impact
  - Advanced Call Distribution – no impact
  - Multi Line Hunt Group – no impact
  - Line State Monitoring – no impact
  - Call Park/Pickup – no impact
- Enhanced Application Features
  - Voicemail – no impact
  - Commportal Web Services – no impact
  - Orecx call media recording – no impact
  - Large Conference – no impact
  - Music on Hold – no impact
  - SIP-TLS and SRTP encryption – no impact
- Call routing services
  - Inbound Local and LD call services – ISUP TDM trunk capacity will be at 50%
  - Outbound Local interconnection Services – ISUP TDM trunk capacity will be at 50%
  - Outbound LD Services – calls will overflow route to Bellevue SIP
  - Toll Free 800 inbound – ISUP TDM trunk capacity will be at 50%
  - Toll Free outbound services – no impact

        - 911 Emergency access – Eastern market E911 will reroute to BW 911
    - Management Services
        - Billing services – no impact
        - Provisioning services – no impact
        - Alarm monitoring services – no impact
        - SAS call logging services – no impact

Legacy network subscribers:

- All services - impact similar to cCFS network

### *Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surviving site?
  Most TDM based voice services on cCFS network are geo-redundant and will use Scottsbluff UMG resources. Eastern market 911 calls will automatically overflow to SIP based Bandwidth 911.
- What applications require manual tasks to complete failover?
    - All cCFS network outbound TDM traffic (accept for 911) will need to diverted to the overflow SIP trunks to free up resources for inbound traffic.
        - Add wildcard LCR routes in translations to divert all outbound traffic to the overflow SIP trunks.

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

These Servers/VMs should be restored in order to recover all Priority 1 and Priority 2 services.

cCFS Network

- Metaswitch UMG Allo-LCN-UMG

### *Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *cCFS Network*

- Allo-LCN-UMG
  No impact for loss of a single CH6010 server instance.
  Similar to Scenario 1 for loss of CH6010 server pair.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan. Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# LNK23 - SON Site Plan

## Scenario 1 – Total Loss of Lincoln State of NE LNK23 SON site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

cCFS network subscribers:

- Basic telephone services
  - Residential analog – no impact
  - Residential VoIP telephone – no impact
  - Business analog – no impact
  - Business VoIP telephone – partial outage for hard-coded State of NE phones, State of NE phones will reregister with SON-BLV-ISC1
  - Enterprise PBX analog interconnection – no impact
  - Enterprise PBX VoIP interconnection – no impact
  - Max UC Desktop and Mobile softphone client – no impact
  - CallerID – no impact
  - Robocall blocking – no impact
  - Call Forwarding – no impact
  - Three-Way Calling – no impact
  - Fax/Data – no impact
  - DTMF Interworking – no impact
- Advanced Business Features
  - Auto Attendant – no impact
  - Advanced Call Distribution – no impact
  - Multi Line Hunt Group – no impact
  - Line State Monitoring – no impact
  - Call Park/Pickup – no impact
- Enhanced Application Features
  - Voicemail – no impact
  - Commportal Web Services – no impact
  - Orecx call media recording – no impact
  - Large Conference – no impact
  - Music on Hold – no impact
  - SIP-TLS and SRTP encryption – no impact
- Call routing services
  - Inbound Local and LD call services – no impact
  - Outbound Local interconnection Services – no impact
  - Outbound LD Services – no impact
  - Toll Free 800 inbound – no impact
  - Toll Free outbound services – no impact
  - 911 Emergency access – no impact
- Management Services
  - Billing services – no impact

- Provisioning services – no impact
- Alarm monitoring services – no impact
- SAS call logging services – no impact

### *Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surviving site?
  Most voice services on the State of NE network will switchover from LNK23 site and run on the Omaha-Bellevue BLV11 site automatically.
- What applications require manual tasks to complete failover?
  - State of NE SIP devices hardcoded to Lincoln will need manual redirect to Bellevue.
    - Configure any State of NE SIP end-user devices (e.g. ADTRAN 600) with simplex SIP proxy servers to point to SON-BLV-ISC1 as needed.

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

All State of NE services should register via SON-BLV-ISC1. These Servers/VMs should be restored on priority basis as necessary.

- cCFS Network
  - Metaswitch Perimeta SBC SON-LCN-ISC1
  - Cisco ASA Firewall SON-LCN-FW

### *Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

## Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *cCFS Network*

- Metaswitch Perimeta SBC SON-LCN-ISC1
  No impact for loss of a single Dell server.
  Similar to Scenario 1 for loss of Dell server pair, SON-BLV-ISC1 will take over for SON-LCN-ISC1.

- Cisco firewall SON-LCN-FW
  No impact for loss of a single Cisco ASA server.
  Similar to Scenario 1 for loss of Cisco ASA server pair, SON-OMA-FW will take over for SON-LCN-FW.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan. Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# SCB01 Site Plan

## Scenario 1 – Total Loss of Scottsbluff Headend SCB01 site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

### *Service impact*

cCFS network subscribers:

- Basic telephone services
  - Residential analog – no impact
  - Residential VoIP telephone – no impact
  - Business analog – no impact
  - Business VoIP telephone – no impact
  - Enterprise PBX analog interconnection – no impact
  - Enterprise PBX VoIP interconnection – no impact
  - Max UC Desktop and Mobile softphone client – no impact
  - CallerID – no impact
  - Robocall blocking – no impact
  - Call Forwarding – no impact
  - Three-Way Calling – no impact
  - Fax/Data – no impact
  - DTMF Interworking – no impact
- Advanced Business Features
  - Auto Attendant – no impact
  - Advanced Call Distribution – no impact
  - Multi Line Hunt Group – no impact
  - Line State Monitoring – no impact
  - Call Park/Pickup – no impact
- Enhanced Application Features
  - Voicemail – no impact
  - Commportal Web Services – no impact
  - Orecx call media recording – no impact
  - Large Conference – no impact
  - Music on Hold – no impact
  - SIP-TLS and SRTP encryption – no impact
- Call routing services
  - Inbound Local and LD call services – ISUP TDM trunk capacity will be at 50%
  - Outbound Local interconnection Services – ISUP TDM trunk capacity will be at 50%
  - Outbound LD Services – calls will overflow route to Bellevue SIP
  - Toll Free 800 inbound – ISUP TDM trunk capacity will be at 50%

        - Toll Free outbound services – no impact
        - 911 Emergency access – Western market E911 will reroute to BW 911
    - Management Services
        - Billing services – no impact
        - Provisioning services – no impact
        - Alarm monitoring services – no impact
        - SAS call logging services – no impact

Legacy network subscribers:

- Basic telephone services
    - Residential analog – no impact
    - Residential VoIP telephone – N/A
    - Business analog – no impact
    - Business VoIP telephone – outage until Metaswitch Perimeta SBC Allo-SCB-ISC1 is restored
    - Enterprise PBX analog interconnection – no impact
    - Enterprise PBX VoIP interconnection – limited outage until Metaswitch Perimeta SBC Allo-SCB-ISC1 is restored
    - Max UC Desktop and Mobile softphone client – N/A
    - Caller ID – no impact
    - Robocall blocking – no impact
    - Call Forwarding – no impact
    - Three-Way Calling – no impact
    - Fax/Data – no impact
    - DTMF Interworking – no impact
- Advanced Business Features
    - Auto Attendant – no impact
    - Advanced Call Distribution – no impact
    - Multi Line Hunt Group – no impact
    - Line State Monitoring – no impact
    - Call Park/Pickup – no impact
- Enhanced Application Features
    - Voicemail – no impact
    - Commportal Web Services – no impact
    - Orecx call media recording – no impact
    - Large Conference – no impact
    - Music on Hold – no impact
    - SIP-TLS and SRTP encryption – no impact
- Call routing services uses cCFS resources
    - Inbound Local and LD call services – ISUP TDM trunk capacity will be at 50%
    - Outbound Local interconnection Services – ISUP TDM trunk capacity will be at 50%
    - Outbound LD Services – calls will overflow route to Bellevue SIP
    - Toll Free 800 inbound – ISUP TDM trunk capacity will be at 50%
    - Toll Free outbound services – no impact
    - 911 Emergency access – Western market E911 will reroute to BW 911

- Management Services
  - Billing services – no impact
  - Provisioning services – no impact
  - Alarm monitoring services – no impact
  - SAS call logging services – no impact

### *Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surviving site?

  cCFS Network
  - Most TDM based voice services on cCFS network are geo-redundant and will use Lincoln UMG resources. Western market 911 calls will automatically overflow to SIP based Bandwidth 911.

  Legacy Network
  - Legacy SIP subscribers and SIP-PBXs using the Allo-SCB-ISC1 Metaswitch Perimeta SBC will be out of service until Allo-SCB-ISC1 is restored or subscribers are migrated to the cCFS Metaswitch Perimeta SBCs in Bellevue and/or Denver.
  - Legacy subscribers requiring UMG DSP resources for DTMF/Fax transcoding will use SCTSNE-UMG located in Scottsbluff CO SCB11 site. Loss of both SCB01 and SCB11 sites will require migration of affected subscribers to cCFS similar to impact to Legacy subscribers for loss of BLV11 site.
- What applications require manual tasks to complete failover?

  cCFS Network
  - All outbound cCFS network TDM traffic (accept for 911) will need to diverted to the overflow SIP trunks to free up resources for inbound traffic.
    - Add wildcard LCR routes in translations to divert all outbound traffic to the overflow SIP trunks.

  Legacy Network
  - All Legacy SIP subscribers and SIP-PBXs using Allo-SCB-ISC1 will require manual migration of affected subscribers by priority to cCFS similar to impact to Legacy subscribers for loss of BLV11 site.
  - Loss of both SCB01 and SCB11 sites will require manual migration of affected DTMF/Fax/Modem subscribers by priority to cCFS similar to impact to Legacy subscribers for loss of BLV11 site.

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

These Servers/VMs should be restored in order to recover all Priority 1 and Priority 2 services.

- Legacy Network
    - Metaswitch Perimeta SBC Allo-SCB-ISC1

- cCFS Network
    - Metaswitch UMG Allo-SCB-UMG

### *Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

## Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *cCFS Network*

- Metaswitch UMG Allo-SCB-UMG
  No impact for loss of a single CH6010 server instance.
  Similar to Scenario 1 for loss CH6010 server pair.

### *Legacy Network*

- Metaswitch Perimeta SBC Allo-SCB-ISC1
  No impact for loss of a single CH6010 server.
  Similar to Scenario 1 for total loss of CH6010 server pair. Full outage for Legacy SIP subscribers using Allo-SCB-ISC1.

- Metaswitch UMG ALNCNE-UMG
  No impact for loss of a single component of UMG2510.
  Similar to Scenario 1 for total loss of UMG2510.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan.  Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol.  *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# SCB11 Site Plan

## Scenario 1 – Total Loss of Scottsbluff CO SCB11 site

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

cCFS network subscribers:

- All services – no impact

Legacy network subscribers:

- All services – no impact

### *Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surviving site?
  Legacy Network
  - Legacy subscribers requiring UMG DSP resources for DTMF/Fax transcoding will use ALNCNE-UMG located in Scottsbluff Headend SCB01 site. Loss of both SCB01 and SCB11 sites will require migration of affected subscribers to cCFS similar to impact to Legacy subscribers for loss of BLV11 site.
- What applications require manual tasks to complete failover?
  Legacy Network
  - Loss of both SCB01 and SCB11 sites will require manual migration of affected DTMF/Fax/Modem subscribers by priority to cCFS similar to impact to Legacy subscribers for loss of BLV11 site.

### *Phase 1 – Infrastructure Replacement*

(Part of Data Center Disaster recovery: site vendor or CI Team)

- Establish physical security
- Power
- HVAC
- (Access/facilities for staff doing the recovery?)

### *Phase 2 – Establish external connectivity*

(Part of Data Center Disaster recovery: ALLO Network Team, Nelnet & facility owner)

### *Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(Part of Data Center Disaster recovery: joint effort with vendors & Nelnet)

### *Phase 4 – Most Critical Servers*

Legacy network will use ALNCNE-UMG for DSP resources. This Server should be restored as necessary.

- Legacy Network
    - Metaswitch SCTSNE-UMG

### *Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Scenario 2.

## Scenario 2 – Server Loss

See Appendix B for individual server restoral process. This section defines the effect on service with individual server loss and method to restore any loss of service.

### *Legacy Network*

- Metaswitch SCTSNE-UMG
  No impact for loss of a single component of UMG3510.
  Similar to Scenario 1 for total loss of UMG3510.

## Testing of plan

Test out services and applications using the Basic cCFS Test Plan. Individual site application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Appendix C.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporate Communications.

# Appendix A: Individual Server Sparing and Availability

This appendix is intended to provide an overview of currently apps/services, and considerations for prioritizing restoral with the available resources. It is expected that each application will capture vendor-specific requirements & other recovery details in its own DR plan.

Risk Tiers:

- Tier 1: Most critical risks based on customer/company impact, including those needed to restore other services.
- Tier 2: Critical services not listed in Tier 1
- Tier 3: Other production systems
- Tier 4: Dev/Lab

Sites:

- BLV11 – TierPoint data center, Bellevue, NE. - Primary data center for Voice services
- DEN11 – 910 Telecom, Denver, CO. - Primary data center for Voice services
- SCB01 – Scottsbluff headend/hub – cCFS TDM Voice services, Legacy VoIP/TDM Voice Services
- SCB11 – Scottsbluff Lumen CO – TDM Voice Services
- LNK01 – Lincoln #1 hub – cCFS TDM Voice Services
- LNK04 – Lincoln #4 – cCFS TDM Voice Services
- LNK23 – State of NE data center – State of NE Voice services
- ALN11 – Alliance Lumen CO – TDM Voice Services

## *cCFS Voice Network*

| Voice Network Element | Server type | Hardware type | Risk Tier | redundancy | Site(s) | HA Arch | Notes |
|---|---|---|---|---|---|---|---|
| Allo-BLV-cCFS-MVS | Metaview MVS | VM | 1 | geo+site | BLV11 | Act/Sby | 12 CPU, 24GB mem, 300GB disk |
| Allo-BLV-AMGC | Metaswitch AMGC | VM | 1 | geo+site | BLV11 | Act/Sby | 12 CPU, 48GB mem, 200GB disk |
| Allo-BLV-CFS | Metaswitch CFS | VM | 1 | geo+site | BLV11 | Act/Act | 12 CPU, 48GB mem, 200GB disk |
| Allo-BLV-ISC2 | Perimeta SBC | VM | 1 | geo+site | BLV11 | Act/Act | 8 CPU, 16GB mem, 40GB disk, PCI passthrough |
| SoN-BLV-ISC1 | Perimeta SBC | Dell R640 | 1 | geo+site | BLV11 | Act/Act | Spare in Lincoln Office |
| Allo-BLV-MVD | Metaview Director | VM | 1 | geo+site | BLV11 | Act/Sby | 4 CPU, 8GB mem, 100GB disk |
| BLV11-FW06 | Cisco Firewall | Cisco ASA | 1 | geo+site | BLV11 | Act/Act | Spare in Lincoln office |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SoN-OMA-FW | Cisco Firewall | Cisco ASA | 1 | geo+site | BLV11 | Act/Act | Spare in Lincoln office |
| Allo-DEN-cCFS-MVS | Metaview MVS | VM | 1 | geo+site | DEN11 | Act/Sby | 12 CPU, 24GB mem, 300GB disk |
| Allo-DEN-AMGC | Metaswitch AMGC | VM | 1 | geo+site | DEN11 | Act/Sby | 12 CPU, 48GB mem, 200GB disk |
| Allo-DEN-CFS | Metaswitch CFS | VM | 1 | geo+site | DEN11 | Act/Act | 12 CPU, 48GB mem, 200GB disk |
| Allo-DEN-EAS | Metasphere EAS | VM | 1 | simplex | DEN11 | None | 12 CPU, 24GB mem, 1000GB disk |
| Allo-DEN-ISC3 | Perimeta SBC | VM | 1 | geo+site | DEN11 | Act/Act | 8 CPU, 16GB mem, 40GB disk, PCI passthrough |
| Allo-DEN-MVD | Metaview Director | VM | 1 | geo+site | DEN11 | Act/Sby | 4 CPU, 8GB mem, 100GB disk |
| DEN11-FW01 | Cisco Firewall | Cisco ASA | 1 | geo+site | DEN11 | Act/Act | Voice-VRF Firewall Managed by Nelnet |
| SoN-LNK-ISC1 | Perimeta SBC | Dell R640 | 1 | geo+site | LNK23 | Act/Act | Spare in Lincoln office |
| SoN-LNK-FW | Cisco Firewall | Cisco ASA | 1 | geo+site | LNK23 | Act/Act | Spare in Lincoln office |
| Allo-BLV-MRS1 | Metaswitch MRS | VM | 2 | geo+site | BLV11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-BLV-MRS2 | Metaswitch MRS | VM | 2 | geo+site | BLV11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-BLV-MRS3 | Metaswitch MRS | VM | 2 | geo+site | BLV11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-BLV-RPAS1 | Metaswitch RPAS | VM | 2 | geo+site | BLV11 | Act/Act | 4 CPU, 4GB mem, 100GB disk |
| Allo-BLV-RPAS2 | Metaswitch RPAS | VM | 2 | geo+site | BLV11 | Act/Act | 4 CPU, 4GB mem, 100GB disk |
| Allo-BLV-ORK1 | OrecX Voice Recorder | VM | 2 | geo+site | BLV11 | Act/Act | 4 CPU, 8 GB Mem, 250 GB Disk |
| Allo-BLV-cCFS-SAS | Metaswitch SAS | VM | 2 | geo+site | BLV11 | Act/Sby | 12 CPU, 24GB mem, 4TB disk |
| Allo-BLV-OBS1 | Metaswitch OBS | VM | 2 | geo+site | BLV11 | Act/Act | 8 CPU, 16GB mem, 100GB disk |
| Allo-DEN-RPAS1 | Metaswitch RPAS | VM | 2 | geo+site | DEN11 | Act/Act | 4 CPU, 4GB mem, 100GB disk |
| Allo-DEN-RPAS2 | Metaswitch RPAS | VM | 2 | geo+site | DEN11 | Act/Act | 4 CPU, 4GB mem, 100GB disk |
| Allo-DEN-cCFS-SAS | Metaswitch SAS | VM | 2 | geo+site | DEN11 | Act/Sby | 12 CPU, 24GB mem, 4TB disk |
| Allo-DEN-OBS1 | Metaswitch OBS | VM | 2 | geo+site | DEN11 | Act/Act | 8 CPU, 16GB mem, 100GB disk |
| Allo-DEN-OBS2 | Metaswitch OBS | VM | 2 | geo+site | DEN11 | Act/Act | 8 CPU, 16GB mem, 100GB disk |
| Allo-LCN-UMG1 | Metaswitch UMG | CH6010 | 2 | geo+site | LNK01 | Act/Sby | Spares via Metaswitch |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ALN11-OPT01 | ADTRAN Multiplexer | Opti | 2 | geo | ALN11 | Act/Act | Spares via ADTRAN |
| Allo-SCB-UMG1 | Metaswitch UMG | CH6010 | 2 | geo+site | SCB01 | Act/Sby | Spares via Metaswitch |
| SCB11-OPT01 | ADTRAN Multiplexer | Opti | 2 | geo | SCB11 | Act/Act | Spares via ADTRAN |
| Allo-BLV-OBS2 | Metaswitch OBS | VM | 3 | geo+site | BLV11 | Act/Act | 8 CPU, 16GB mem, 100GB disk |
| Allo-BLV-DCM1 | Metaswitch DCM | VM | 3 | geo+site | BLV11 | Act/Act | 1 CPU, 1 GB Mem, 10 GB Disk |
| Allo-BLV-DCM2 | Metaswitch DCM | VM | 3 | geo+site | BLV11 | Act/Act | 1 CPU, 1 GB Mem, 10 GB Disk |
| Allo-DEN-MRS1 | Metaswitch MRS | VM | 3 | geo+site | DEN11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-DEN-MRS2 | Metaswitch MRS | VM | 3 | geo+site | DEN11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-DEN-MRS3 | Metaswitch MRS | VM | 3 | geo+site | DEN11 | Act/Act | 8 CPU, 8GB mem, 100GB disk |
| Allo-DEN-DCM1 | Metaswitch DCM | VM | 3 | geo+site | DEN11 | Act/Act | 1 CPU, 1 GB Mem, 10 GB Disk |
| Allo-DEN-DCM2 | Metaswitch DCM | VM | 3 | geo+site | DEN11 | Act/Act | 1 CPU, 1 GB Mem, 10 GB Disk |
| Allo-DEN-N-Series | Metaswitch N-Series | VM | 3 | simplex | DEN11 | None | 4 CPU, 8GB mem, 300GB disk |

## *Legacy Voice Network*

| Voice Network Element | Server type | Hardware type | Risk Tier | redundancy | Site(s) | HA Arch | Notes |
|---|---|---|---|---|---|---|---|
| Allo-BLV-MVS1 | Metaview MVS | VM | 1 | site-redundancy | BLV11 | Act/Sby | 12 CPU, 24GB mem, 300GB disk |
| Allo-CA1 | Metaswitch CFS | VM | 1 | site-redundancy | BLV11 | Act/Sby | 4 CPU, 8GB mem, 200GB disk |
| OMAHA-EAS | Metasphere EAS | VM | 1 | none | BLV11 | Act/Act | 4 CPU, 8GB mem, 300GB disk |
| Allo-Omaha-MVD-1 | Metaview Director | VM | 1 | site-redundancy | BLV11 | Act/Sby | 4 CPU, 8GB mem, 100GB disk |
| ALNCNE-UMG | Metaswitch UMG | UMG2510 | 1 | geo+site | SCB01 | Act/Act | Spares via 3rd party vendor |
| SCB-ISC1 | Perimeta SBC | CH6010 | 1 | site-redundancy | SCB01 | Act/Sby | Spares via Metaswitch |
| SCTSNE-UMG | Metaswitch UMG | UMG3510 | 1 | geo+site | SCB11 | Act/Act | Spares via 3rd party vendor |
| OMAHA-N-Series | Metaswitch N-Series | VM | 2 | none | BLV11 | Act/Sby | 4 CPU, 8GB mem, 300GB disk |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| BLV11-FW01 | Cisco firewall | Cisco ASA | 2 | site-redundancy | BLV11 | Act/Sby | Spare in Lincoln office |
| ALLO-BLV11-SAS | Metaswitch SAS | VM | 2 | none | BLV11 | None | 4 CPU, 8GB mem, 1000GB disk |
| Allo-DCM1 | Metaswitch DCM | VM | 3 | site-redundancy | BLV11 | Act/Sby | 1 CPU, 1GB mem, 10GB disk |
| Allo-DCM2 | Metaswitch DCM | VM | 3 | site-redundancy | BLV11 | Act/Sby | 1 CPU, 1GB mem, 10GB disk |
| Allo-DNV-MVS2 | Metaview MVS | VM | 3 | site-redundancy | BLV11 | Act/Sby | 12 CPU, 24GB mem, 300GB disk |

# Appendix B: Individual Server Restoral Process (additional details needed)

This section provides instructions on restoring the software and configuration data on an individual Metaswitch network element that has suffered a system failure.

## *Metaswitch VM Instances*

Ensure VM resources are available for VM Instance. If needed and as per the Data Center Disaster Recovery Plan, repair/install server and SAN hardware and establish VMware environment.

Restore VM with mirrored VM backup if available. If backup is not available VM will need to be recommissioned per the respective server Metaswitch Operations and Procedures manual. If this is the first server to be restored of a mated pair, the server will need to be commissioned and configuration restored from backup. If this is the second server to be restored of the mated pair, this server will be partnered with the running server.

## *Metaswitch Perimeta SBC Dell R640 server*

Physically replace faulty Dell R640 server with spare Dell R640 server located in Lincoln. Refer to *Metaswitch Perimeta Configuration and Management Guide* for bootstrapping process.

If this is the first server to be restored of the mated pair, this server will need to be commissioned and configuration installed from backup. If this is the second server to be restored of the mated pair, this server will be partnered with the running server.

## *Metaswitch Perimeta SBC CH6010 server*

Order replacement CH6010 parts from Metaswitch and physically replace faulty parts. Refer to *Metaswitch Perimeta Configuration and Management Guide* for bootstrapping process.

If this is the first server to be restored of the mated pair, this server will need to be commissioned and configuration installed from backup. If this is the second server to be restored of the mated pair, this server will be partnered with the running server.

## *Metaswitch Perimeta SBC CH6010 server*

Order replacement CH6010 parts from Metaswitch and physically replace faulty parts. Refer to *Metaswitch Perimeta Configuration and Management Guide* for bootstrapping process.

If this is the first server to be restored of the mated pair, this server will need to be commissioned and configuration installed from backup. If this is the second server to be restored of the mated pair, this server will be partnered with the running server.

## *Appendix C: FCC/PUC/PSC Communications (additional details needed)*

Customer operations is responsible for all customer, federal and state communications regarding network outages.

Additional details to follow.

## *Appendix D: Outstanding questions/action items*

- Appendix B details – in progress
- Appendix C details – in progress
- AMGC requires manual switchover - in progress
- CFS subscriber Rehoming Allowed audit – in progress
- MVWeb user audit.  Allo-BLV-MVS/Allo-DEN-MVS synchronization
- VPN access to Denver MVS during Voice-VRF BLV11-FW06 firewall outage
- MVWeb access via DNS-SRV instead of IP address
- EAS Auto-Attendant temporary warm backup solution
- Metaswitch EAS SSS geo-redundancy – Q3 2021 - requires Cisco UCS resources and Metaswitch bake-in scheduled for Q3
- N-Series Conferencing/MOH warm backup process
- Geo-redundant storage of backups

*Data Center*

# ALLO Data Center Infrastructure Disaster Recovery Plan [DRAFT]

## Overview & Scope

This DR plan focuses on restoring ALLO service provider data center infrastructure so that various SP applications/services can be restored. Each application will have its own specific DR plan.

The primary data center locations are as follows. Note that these facilities are both operated by third-party vendors, not the ALLO CI team:

- BLV11 – TierPoint data center, Bellevue, NE. Primary data center
- DEN11 – 910 Telecom, Denver, CO. Backup data center (not all services)

Tertiary facilities of interest supporting SP services (most are operated by ALLO):

- HST01 – Hastings hub (Speedtest server)
- SCB01 – Scottsbluff headend/hub (Speedtest server, NTP servers, Vaonet, Legacy DHCP)
- LNK04 – Lincoln #4 hub (NTP servers, voice UMG)
- SCB11(?) – Scottsbluff CO (legacy voice UMG); *note that this is a 3rd-party facility*
- LNK11 – NDC Lincoln facility (Speedtest server); *note that this is a 3rd-party facility*

## Assumptions

- Equipment for recovery efforts such as laptops, KVMs, etc. will be available at work site(s).
- Supporting IT systems will be accessible to provide access to critical documentation, system credentials, license keys, and tools such as e-mail.
- Safety and security of associates takes priority over recovery activities.
- In an extensive disaster event staff & equipment resources may be insufficient, which in turn will prolong recovery activities.
- Depending on the severity of the incident, customers and other ALLO teams may be required to modify their operations to accommodate differences in applications/services until a full recovery has been completed. This may include manual processing for an extended period of time.

# Sparing/Availability

Spares are not currently stocked for most components. Replacements provided by vendor support agreements. Also, SAN arrays and Metaswitch voice core are remotely monitored by their respective vendors.

# Plan

## Scenario 1 – Total Loss of Primary or Secondary Data Center

### *Disaster Assessment*

- What is salvageable?
- What needs to be ordered for equipment?

*Phase 0 – Execute or Confirm Application Failover*

- What applications/services can run on the surving site?
- What applications require manual tasks to complete failover?

*Phase 1 – Infrastructure Replacement (site vendor or CI Team)*

- Establish physical security
- Power
- HVAC
- (access/facilities for staff doing the recovery?)

*Phase 2 – Establish external connectivity*

(ALLO Network Team, Nelnet & facility owner)

*Phase 3 – Repair/install server & SAN hardware and establish VMware environment*

(joint effort with vendors & Nelnet)

*Phase 4 – Most Critical VMs*

These VMs are needed to support most/all application or service restorals.

- Site-specific UCS Central VM (BLV11 only)
- Site-specific vCenter
- <site>-bkp01 – Backup storage (images, configuration files, etc.)
- <site>-ops01 – Local bastion host. May not need if surviving site bastion can be used.
- Nelnet CommVault (off-site backups, if available) located outside SP environment

*Phase 5 – Recover specific applications*

Will require prioritizing due to expected limited staff & network resources. See also Appendix A.

## Scenario 2 – Server Loss

Similar to Scenario 1, except surving data center blades may be partially retasked to support most critical services.

## Scenario 3 – Complete loss of one or more SAN volume(s)

This is similar to Scenario 1, but could include catatrophic conditions that place SAN in read-only mode, volume corruption due to software failure, or ransomware encryption attacks.

Identify whether hardware, software, or other problem. In some cases hardware replacement may not be necessary, and recovery can be facilitated via SAN snapshots or off-site backups.

Initial triage analysis MUST identify if incident indicates ransomware or other malware, as this may render any backups unusable.

## Resources required (internal, 3rd party)

- Data Center vendor team(s)
- Nelnet UCS/SAN/VMware resources (Ben Fry team)

- Nelnet DC & CommVault team (Brian Galvin team)
- ALLO Core/Transport Network team
- ALLO Application-specific teams & app vendor support

## Testing of plan

Test using tabletop exercises. Individual application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *FCC/PUC/PSC Communications*

See Voice Services plan

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of CorporateCommunications.

## Appendix A: Application Restoral Strategy

This appendix is intended to provide an overview of currently apps/services, and considerations for prioritizing restoral with the available resources. It is expected that each application will capture vendor-specific requirements & other recovery details in its own DR plan.

Risk Tiers:

- Tier 1: Most critical risks based on customer/company impact, including those needed to restore other services.
- Tier 2: Critical services not listed in Tier 1
- Tier 3: Other production systems
- Tier 4: Dev/Lab

| App Category | App or Service | Risk Tier | Description | Owner | Site(s) | HA Arch | Notes |
|---|---|---|---|---|---|---|---|
| UCS-SAN-VMware | vCenter | 1 | VMware management | Nelnet | BLV11<br>DEN11<br>~~SCB01~~ | Actv/Actv | For BLV/DEN: Can manage both sites from either vCenter in normal state, may be able to manage from surving vCenter. SCB01 node is ESXi-only, unmanaged |
| Backup | Backup VM | 1 | Storage VM for config & images | Sys Engr | BLV11 | No | Data to restore other apps |
| Remote Access | Site bastion | 1 | General mgmt. jump host (SSH) | Sys Engr | BLV11<br>DEN11 | Actv/Actv | Defer recovery if other site can be used |
| DDI | Recursive DNS (Mgmt Net) | 1 | Recursive DNS for internal & Management VRF | Sys Engr | BLV11<br>DEN11 | Actv/Actv | Used by internal servers, not customer-facing |
| DDI | Recursive DNS (Public Net) | 2 | Customer-facing DNS, also used by many applications | Sys Engr | BLV11<br>DEN11 | Actv/Actv | Not purely recursive (special rules for IPTV and Speedtest) |
| DDI | Authoritative DNS | 2 | Internal & external authoritative DNS zones (incl customers) | Sys Engr | BLV11<br>DEN11 | Actv/Actv | Has both on-prem zones & AWS-hosted (Route53 service). Critical for Voice & IPTV services. |
| DDI | DHCP | 2 | Customer-facing DHCP (BLV,DEN) | Sys Engr | BLV11<br>DEN11 | Actv/Actv* | Requires manual intervention if extended downtime (partner down state) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DDI | DHCP | 2 | Legacy DHCP (SCB) | Sys Engr | SCB01 | None | Instance is not recoverable. Customers must be migrated to main DHCP and/or new VLANs |
| DDI | IPAM | 2 | DDI management & REST API | Sys Engr | BLV11<br>DEN11 | Actv/Stby | Requires manual failover of DNS entry |
| Backup | Katello/Foreman | 2 | Platform for automating server (re)builds & patching | Sys Engr | BLV11 | None | Cannot automate all types of server builds |
| NTP | NTP | 2 | NTP for Mangement VRF & DC | Engr | BLV11<br>DEN11<br>LNK04 | Actv/Actv | |
| NTP | NTP | 2 | Customer-facing NTP, also used by some services | Engr | BLV11<br>DEN11 | Actv/Actv | |
| Voice | Legacy Voice | 2 | Metaswitch (legacy virtual) | Voice Engr, Net Engr, Nelnet | BLV11<br>SCB01<br>SCB11 | (limited) | Single site, some components within the BLV11 VMware environment provide HA |
| Voice | Voice (cCFS) | 2 | Clustered Metaswitch (Adtran OPTI, Orecx, Equinox, Cisco FW, Syniverse, Neustar, AWS/Mitel VKS, et al) | Voice Engr, Sys Engr, Net Engr, Nelnet | BLV11<br>DEN11<br>LNK04<br>SCB01 | (partial) | Cannot support HA for all customers on all services at this time. Legacy voice migration & EAS-SSS projects will address the most critical gaps. |
| Monitoring | Splunk | 3 | Splunk | Sys Engr | BLV11 | None | Critical for some monitoring |
| EMS-OSS | Calix CMS | 3 | CMS | Sys Engr | BLV11<br>DEN11 | Actv/Stby | Requires manual data load & failover |
| EMS-OSS | Calix SMx | 3 | SMx | Sys Engr | BLV11 | None | |
| EMS-OSS | Infinera NMS | 3 | TNMS | Sys Engr | BLV11 | None | |
| EMS-OSS | Vaonet | 3 | Vaonet monitoring | Sys Engr | SCB01<br>(BLV11?) | None | Application backups only, VMware env may not be recoverable |
| EMS-OSS | Xymon | 3 | Xymon monitoring | Sys Engr | BLV11 | None | |
| EMS-OSS | Cacti | 3 | Cacti (performance metrics) | Sys Engr | BLV11 | None | |
| EMS-OSS | Agent Portal (and other apps?) | 3 | Agent Portal & Database node | SIG | BLV11 | None | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Backup | TFTP | 3 | Config file storage | Sys Engr | BLV11 | None | |
| Remote Access | RADIUS/TACACS | 3 | Device mgmt. access | Sys Engr | DEN11 (BLV11*) | Actv/Actv | Pending license for 2nd site |
| EMS-OSS | Ocular IP | 3 | Ocular IP | Sys Engr | DEN11 | None | |
| EMS-OSS | Skylight | 3 | Accedian Skylight | Sys Engr | DEN11 | None | |
| Monitoring | Fujitsu VPN | 3 | EMS event feed to Fujitsu | Sys Engr | BLV11<br>DEN11 | Actv/Actv | |
| DDoS | Arbor | 3 | DDoS mitigation | Sys Engr | SCB01 (BLV11*) | None | Currently on h/w appliance in SCB01. *Will migrate to VM in DC in 2021 |
| Security | Cisco FMC | 3 | Firewall policy | Sys Engr | BLV11 | None | |
| Mail | SMTP Relay | 3 | Customer-facing relay | Sys Engr | BLV11<br>DEN11 | Actv/Actv | Also critical for some monitoring/alerting |
| CGN | CGN Logging | 3 | CGN logs for legal compliance | Sys Engr | BLV11 | None | Uses on-prem & AWS services |
| Speedtest | Speedtest | 3 | Ookla Speedtest servers | Sys Engr | SCB01<br>DEN11<br>LNK11<br>HST01 | None | Servers do not provide failover |
| IPTV | IPTV | 3 | ALLO in-house Mediaroom infr. | Video/Sys | BLV11 | None | Some components known to be EOL |
| Lab | Lab | 4 | Lab systems | Sys Engr | BLV11<br>DEN11 | None | May need to leave offline to free resources |

*Production Network (Core)*

# ALLO Core Network Disaster Recovery Plan

## Overview & Scope

This DR plan focuses on restoring ALLO service provider core network infrastructure, transport, and peering relationsips so that full network capacity and protection can be restored. Each backbone site will have its own specific DR plan.

The primary data center locations are as follows. Note that some of these facilities are operated by third-party vendors, as well as some operated by the ALLO CI team:

- OMA11 – 1623 Farnam Datacenter, Omaha, NE
- DEN11 – 910 Telecom, Denver, CO
- SCB01 – Scottsbluff Head End, Scottsbluff, NE
- LNK11 – Lincoln Datacenters, Lincoln, NE

## Assumptions

- Equipment for recovery efforts such as laptops, KVMs, etc. will be available at work site(s).
- Supporting IT systems will be accessible to provide access to critical documentation, system credentials, license keys, and tools such as e-mail.
- Safety and security of associates takes priority over recovery activities.
- In an extensive disaster event staff & equipment resources may be insufficient, which in turn will prolong recovery activities.

# Sparing/Availability

We shelf stock spares for each of these locations at or within 1 hour of the facility. We shelf spare all Allo owned hardware at a minimum of 3%. In the event of a critical disaster, there will not be sufficient spares to rebuild all equipment at impacted location. Additionally, we do not have spares for any vendor provided gear, such as Netflix Cache, Google Cache, or Facebook Cache.

# Impact

Theoretically, the loss of any one of these facilities would not result in customers hard down, with the exception of Papillion, Scottsbluff/Gering, Ashland, or any customers physically terminating in the impacted COLO. However the loss of one of these facilities will greatly impact local/direct peering, cache capacity, as well as egress DIA.

# Plan

## Scenario 1 – Total Loss of backbone site (tornado, flood, fire)

### *Disaster Assessment*

- What is salvageable?
- What equipment do we need to order to fully rebuild site?
- What transport/peering vendors do we need to coordinate restoration efforts with?
- What content providers to we need to contact for hardware replacement?

*Phase 0 – Confirm network failover/stability*

- Ensure all traffic has successfully failed to other transit links/peers/CDN's.
- Monitor capacity/utilization of peers and transit links, balance traffic as/if needed.
- Move individual customer circuits to alternate datacenter to restore services as applicable.

*Phase 1 – Infrastructure Replacement (site vendor or CI Team)*

- Establish physical security.
- Racks
- Power (UPS/Rectifier/PDU/Fuse Panels).
- HVAC
- Fiber restoration to our cage/rack by Allo OSP and/or datacenter staff from MMR.

*Phase 2 – Repair/install new routing/switching hardware*

- Using shelf spares, install minimal hardware in a modified configuration to restore backbone, peering, and market diversity.
    - Network Engineering will provide modified design based of hardware available, severity of damage, and lead times of hardware orders.
    - Likely have to pull hardware from multiple spare locations to complete this, putting them at risk of not having shelf spare in the event of hardware failure.
    - This would be a minimal, temporary configuration, enough to get core links/peering up to provide basic diversity to the network.
- Backups for all gear are stored on the Rancid or FTP server, based off backup type.

*Phase 2 – Establish external connectivity*

- Work with transport providers to restore all backbone circuits.
- Work with peers to bring core peering/DIA back online.
- Work with Allo OSP/transport providers to restore diversity to impacted markets.

*Phase 4 – Final Restoration*

- Remove temporary router/switch configuration and replace with new hardware in original state
- Install/turn up CDN appliances, working with content provider to commission.

## Scenario 2 – Partial loss of site (Vandalism, Malicious act)

Same process as scenario 1, however instead of installing temporary solution, we would do our best to restore full redundancy to site as needed. For the interim, we may shift customers to diverse hardware to get them online while we are working on full restoration.

## Scenario 3 – Single element loss (basic hardware failure)

We have shelf spares at 4 sparing depot locations across the network (Lincoln, North Platte, Scottsbluff, Denver) which are audited by dedicated staff monthly. NTAC monitors these audits, and ensures sparing inventory database (lives on Sharepoint) is accurate. These locations contain a minimum of 3% of deployed hardware for the markets they are responsible for available for dispatch to restore any single element failure. We maintain RTF support on all these spares, so backfill of used spare will be replaced in approximately a 3 week window.

## Resources required (internal, 3rd party)

- Data Center vendor team(s)
- Allo HUB Techs
- Allo Network Engineering
- Allo Systems Engineering
- Allo Critical Infrastrure Team
- Transport carriers (various)
- Peers (various)
- CDN providers (various)
- NOTE – we maintain list of vendors and contacts on Sharepoint.

## Testing of plan

Test using tabletop exercises. Individual application plans tested separately.

## Communication Plan

### *Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

### *Vendor Communications*

Directly with facilities & equipment vendors as required.

### *External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporated Communications.

# *Production Network (Aggregation)*

# ALLO Aggregation Network Disaster Recovery Plan

## Overview & Scope

This DR plan focuses on restoring ALLO service provider aggregation network infrastructure, as well as customer access hardware to fully restore customer services.

## Assumptions

- Equipment for recovery efforts such as laptops, KVMs, etc. will be available at work site(s).
- Supporting IT systems will be accessible to provide access to critical documentation, system credentials, license keys, and tools such as e-mail.
- Safety and security of associates takes priority over recovery activities.
- In an extensive disaster event staff & equipment resources may be insufficient, which in turn will prolong recovery activities.

# Sparing/Availability

We shelf stock spares for each of these locations at or within 4 hours of the facility. We shelf spare all Allo owned hardware at a minimum of 3%. In the event of a critical disaster, there will not be sufficient spares to rebuild all equipment at impacted location.

# Plan

## Scenario 1 – Total Loss of HUB site (tornado, flood, fire)

### *Disaster Assessment*

- What is salvageable?
- What equipment do we need to order to fully rebuild site (routers, switches, optics, access gear, fiber jumpers, fuse panels, etc)?

### *Phase 1 – Infrastructure Replacement (Allo CI and Allo OSP Teams)*

- Establish physical security.
- Racks
- Power (UPS/Rectifier/PDU/Fuse Panels).
- HVAC
- Fiber restoration by Allo OSP.

### *Phase 2 – Repair/install new routing/switching/access hardware*

- Using shelf spares, install minimal hardware in a modified configuration to HUB connectivity (likely not diverse).
    - Network Engineering will provide modified design based of hardware available, severity of damage, and lead times of hardware orders.
    - Likely have to pull hardware from multiple spare locations to complete this, putting them at risk of not having shelf spare in the event of hardware failure.
    - This would be a minimal, temporary configuration, enough to get dedicated and key GPON customers back online.
- Backups for all gear are stored on the Rancid, CMS, or FTP server, based off backup type.

*Phase 2 – Establish external connectivity*

- Work with Allo OSP Team to restore all backbone fiber to HUB.
- Work with Allo OSP Team to restore distribution and feeder routes.

*Phase 4 – Final Restoration*

- Remove temporary router/switch configuration and replace with new hardware in original state
- Install/turn up CDN appliances, working with content provider to commission.

## Scenario 2 – Partial loss of site (Vandalism, Malicious act)

Same process as scenario 1, however instead of installing temporary solution, we would do our best to restore full redundancy to site as needed. For the interim, we may shift customers to diverse hardware to get them online while we are working on full restoration.

## Scenario 3 – Single element loss (basic hardware failure)

We have shelf spares at 4 sparing depot locations across the network (Lincoln, North Platte, Scottsbluff, Denver) which are audited by dedicated staff monthly. NTAC monitors these audits, and ensures sparing inventory database (lives on Sharepoint) is accurate. These locations contain a minimum of 3% of deployed hardware for the markets they are responsible for available for dispatch to restore any single element failure. We maintain RTF support on all these spares, so backfill of used spare will be replaced in approximately a 3 week window.

## Resources required (internal, 3rd party)

- Allo HUB Techs
- Allo Network Engineering
- Allo Systems Engineering
- Allo Critical Infrastrure Team
- NOTE – we maintain list of vendors and contacts on Sharepoint.

## Testing of plan

Test using tabletop exercises. Individual application plans tested separately.

## Communication Plan

*Internal Communications:*

During a service impacting event we will follow the standard incident management protocol. *(Link to the current process here)*

*Vendor Communications*

Directly with facilities & equipment vendors as required.

*External Communications*

During a service impacting event we will follow the standard incident management protocol.

No information should be released to news outlets without prior approval of Corporated Communications