



December 17, 2020

Chief, Foreign Investment Review Section (FIRS)
Deputy Chief, Compliance and Enforcement (FIRS)
On Behalf of the Assistant Attorney General for National Security
United States Department of Justice
National Security Division
175 N Street, NE
Washington, DC 20530
Compliance.Telecom@usdoj.gov

Subject: Frontier Communications Corporation and subsidiaries, FCC File Nos. ISP-PDR-20200624-00005; ITC-ASG-20200625-00095; ITC-ASG-20200625-00096; ITC-ASG-20200625-00097; ITC-ASG-20200625-00098; ITC-ASG-20200625-00099; ITC-ASG-20200625-00100; ITC-ASG-20200625-00102; ITC-ASG-20200625-00103; ITC-ASG-20200625-00104; ITC-ASG-20200625-00105; ITC-ASG-20200625-00106; ITC-ASG-20200625-00107; ITC-ASG-20200625-00108; ITC-ASG-20200625-00109; WC Docket No. 20-197, (TT 20-025 to -040); Applications for Consent to Assign and Transfer Control of Domestic and International Section 214 Authorizations and Authorization to Exceed the 25 Percent Foreign Investment Benchmark.

Dear Sir/Madam:

This Letter of Agreement (“LOA” or “Agreement”) sets forth the commitments that Frontier Communications Corporation and its wholly owned operating subsidiaries¹ (collectively, “Frontier”) make to the U.S. Department of Justice (“USDOJ”), including the Federal Bureau of Investigation (“FBI”), to address national security and law enforcement risks arising from Frontier’s above-referenced applications to the Federal Communications Commission (“FCC”) requesting consent to assign and transfer control of domestic and international Section 214 authorizations pursuant to Section 214 of the Communications Act of 1934, as amended, 47 U.S.C. § 214, and the implementing regulations at 47 C.F.R. §§ 63.04, 63.18, and 63.24, and authorization to exceed the 25 percent foreign investment benchmark

¹ Frontier’s subsidiaries include Citizens Telecommunications Inc.; Commonwealth Telephone Enterprises, LLC; Frontier California Inc.; Frontier Communications of America, Inc.; Frontier Communications of the Carolinas Inc.; Frontier Communications of the Southwest Inc.; Frontier Communications Online and Long Distance Inc.; Frontier Florida LLC; Frontier Mid-States Inc.; Frontier North Inc.; Frontier Southwest Incorporated; Frontier West Virginia Inc.; GVN Services d/b/a Global Valley Long Distance; Ogden Telephone Company; and SNET America, Inc.

pursuant to Section 310 of the Communication Act, 47 U.S.C. § 310 and 47 C.F.R. § 1.5000(a)(1) (“FCC Applications”).

Frontier certifies as true and correct, under penalties outlined in 18 U.S.C. § 1001, all statements Frontier or its representatives have made to USDOJ, the Department of Homeland Security, the Department of Defense, and the FCC in the course of the review of the above-referenced application that was conducted pursuant to Executive Order 13913, 85 Fed. Reg. 19643 (Apr. 8, 2020), and it hereby adopts those statements as the basis for this LOA.

Definitions

1. For purposes of this LOA, the following definitions apply:
 - a. “Access” means: (1) to enter a location, or (2) to obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise view data or systems in any form, including through information technology (IT) systems, cloud computing platforms, networks, security systems, and equipment (software and hardware). For the avoidance of doubt, Access shall be construed broadly to include rather than exclude considered conduct.
 - b. “Call Detail Record” (“CDR”) means the data records or call log records that contain information about each call made by a user and processed by switch, call manager, or call server.
 - c. “Customer Proprietary Network Information” (“CPNI”) means as set forth in 47 U.S.C. § 222(h)(1).
 - d. “Date of FCC Approval” means the date on which the FCC publicly releases approval of the FCC Applications.
 - e. “Date of this LOA” means the date on which Frontier executes this LOA.
 - f. “Domestic Communications” (“DC”) means:
 - i. Wire Communications, or Electronic Communications (whether stored or not), from one location within the United States, including its territories, to another location within the United States; or
 - ii. The U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States or its territories.
 - g. “Domestic Communications Infrastructure” (“DCI”) means:
 - i. Any Frontier system that supports any communications originating or terminating in the United States, including its territories, including any transmission, switching, bridging, and routing equipment, and any associated software (with the exception of commercial-off-the-shelf

(“COTS”) software used for common business functions, *e.g.*, Microsoft Office) used by, or on behalf of², Frontier to provide, process, direct, control, supervise, or manage DC;

h. “Electronic Surveillance” means:

- i. The interception of wire, oral, or electronic communications as set forth in 18 U.S.C. § 2510(1), (2), (4) and (12), respectively, and electronic surveillance as set forth in 50 U.S.C. § 1801(f);
- ii. Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.;
- iii. Acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as set forth in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.;
- iv. Acquisition of location-related information concerning a subscriber or facility;
- v. Preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and
- vi. Access to or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (i) through (v) above and comparable state laws.

i. “Foreign” means non-United States, or its territories.

j. “Government” means any government, or governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision, and any court, tribunal, judicial or arbitral body.

k. “Lawful U.S. Process” means U.S. federal, state, or local court orders, subpoenas, warrants, processes, directives, certificates or authorizations, and other orders, legal process, statutory authorizations and certifications for Electronic Surveillance, physical search and seizure, production of tangible things or Access to or disclosure of DC, call-associated data, transactional data, Subscriber Information, or associated records.

l. “Managed Network Service Provider” or “MNSP” means any third party that has Access to Principal Equipment for the purpose of:

² The phrase “on behalf of,” as used in this paragraph, does not include entities with which Frontier has contracted for peering, interconnection, roaming, long distance, wholesale network access, or other similar arrangements.

- i. network operation; provisioning of Internet and telecommunications services; routine, corrective, and preventative maintenance, including switching, routing, and testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, creation and implementation of modifications or upgrades; or
 - ii. provision of DC or operation of DCI, including: customer support; Operations Support Systems (“OSS”); Business Support Systems (BSS); Network Operations Centers (“NOCs”); information technology; cloud operations/services; 5G (SDN, NFV, Applications); and datacenter services and operations.
- m. “Network Operations Center” or “NOC” means any locations and facilities performing network management, monitoring, accumulating accounting and usage data, maintenance, user support, or other operational functions for DC.
- n. “Offshore” means performing obligations of this LOA using entities and personnel outside of the territorial limits of the United States, whether or not those entities or personnel are employees of Frontier.
- o. “Outsource” means, with respect to DC, supporting the services and operational needs of Frontier at issue in this LOA using contractors or third parties.
- p. “Personally Identifiable Information” or “PII” means any information that uniquely identifies and correlates to a natural person or can be used to distinguish or trace a natural person’s identity, alone, including his or her name, social security number, or biometric records, or when combined with other personal or identifying information that is linked or linkable to a specific individual, including date and place of birth, or parent's surname.
- q. “Principal Equipment” means all primary telecommunications and information network equipment (*e.g.*, hardware, software, platforms, OS, applications, protocols) that supports core telecommunications or information services, functions, or operations of Frontier.
- r. “Security Incident” means:
- i. Any known or suspected breach of this LOA, including a violation of any approved policy or procedure under this LOA;
 - ii. Any unauthorized Access to, or unauthorized disclosure of, PII or Sensitive Personal Data;
 - iii. Any unauthorized Access to, or unauthorized disclosure of, information obtained from or relating to Government entities; or

- iv. Any one or more of the following which affect Frontier’s computer network(s) or associated information systems:
 - A. Unplanned disruptions to a service or denial of a service;
 - B. Unauthorized processing or storage of data;
 - C. Unauthorized modifications to system hardware, firmware, or software; or
 - D. Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect company’s ability to comply with the terms of this LOA.

s. “Sensitive Personal Data” means sensitive personal data as set forth in 31 C.F.R. § 800.241.

t. “Subscriber Information” means any information of the type referred to and accessible subject to the procedures set forth in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

u. “U.S. Records” means Frontier’s customer billing records, Subscriber Information, PII, Sensitive Personal Data, CDRs, CPNI, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by Frontier within the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. § 2703(c), (d) and 18 U.S.C. § 2709.

Personnel

2. Frontier agrees to designate and maintain a U.S. law enforcement point of contact (“LEPOC”) in the United States who will be subject to prior approval by USDOJ, including the FBI. The LEPOC shall be a U.S. citizen residing in the United States or its territories unless USDOJ otherwise agrees in writing. The LEPOC must be approved by USDOJ to receive service of Lawful U.S. Process for U.S. Records and, where possible, to assist and support lawful requests for surveillance or production of U.S. Records by U.S. federal, state, and local law enforcement agencies.

3. Frontier agrees to provide the LEPOC’s PII to USDOJ within 15 days of the Date of FCC Approval. USDOJ agrees to object or waive objection to the LEPOC within 15 days from receiving the LEPOC’s PII.

4. Frontier agrees to notify USDOJ, including the FBI, in writing at least 30 days prior to modifying its LEPOC for USDOJ and FBI objection or non-objection. For those cases involving the unexpected firing, resignation, or death of LEPOC, written notice will be provided within five days of such event. In any of these circumstances, USDOJ and FBI will object or not object to the replacement LEPOC within 30 days of notification.

5. Frontier agrees that the designated LEPOC will have Access to all U.S. Records, and, in response to Lawful U.S. Process, will make such records available in a manner and time consistent with the Lawful U.S. Process.

6. Frontier agrees to implement, either directly or through a vendor, a process to screen newly hired Frontier personnel or any personnel of an approved Outsourced or Offshored service provider performing under an agreement with Frontier that have Access to Frontier's network or U.S. Records. To satisfy its obligation under this Paragraph with respect to the personnel of Outsourced or Offshored service providers, Frontier agrees to commit contractually that such Outsourced or Offshored service providers must comply with the personnel screening process set forth in this Paragraph. The personnel screening process shall include background investigations, public criminal records checks, or other analogous means to ascertain a person's trustworthiness. Frontier further agrees to provide USDOJ with a written description of this personnel-screening process no later than 60 days after the Date of FCC Approval for USDOJ objection or non-objection.

Lawful U.S. Process and Requests for Information

7. Frontier agrees to comply with all applicable lawful interception statutes, regulations, and requirements, as well as comply with all court orders and Lawful U.S. Process for lawfully authorized Electronic Surveillance. Frontier further agrees to certify to USDOJ its compliance with the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001-1010, and its implementing regulations, within 30 days from the Date of FCC Approval.

8. Frontier agrees to provide notice of any material modification to its lawful intercept capabilities to USDOJ within 30 days of such modification, and will re-certify its compliance with CALEA no more than 60 days following its notice to USDOJ of any material new facilities, services, or capabilities.

9. Frontier agrees to comply with all court orders and Lawful U.S. process, including process relating to Electronic Surveillance.

10. Upon receipt of any Lawful U.S. Process, Frontier agrees to place any and all information responsive to the Lawful U.S. Process within the territorial boundaries of the United States and otherwise provide such responsive information to the requesting officials, in a manner and time consistent with the Lawful U.S. Process.

11. Frontier agrees not to provide, or otherwise allow the disclosure of, or Access to, U.S. Records, Domestic Communications, or any call content or call data information, to any Foreign Government or any Foreign person who has not been screened or is otherwise exempt from screening as set forth in Paragraph 6 above ("Unauthorized Foreign Person"), without prior written consent of USDOJ, or a court of competent jurisdiction in the United States, provided that nothing in this provision shall be construed to prevent Frontier from allowing users to access their own account information through standard access tools or customer care requests.

12. Frontier agrees not to disclose the receipt of Lawful U.S. Process, or compliance with Lawful U.S. Process, to any Foreign Government, or any person not authorized under the Lawful U.S. Process, without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

13. Frontier agrees to refer any requests for information described in Paragraph 11, including any legal process from a Foreign Government, to USDOJ as soon as possible, but in no event later than five days after such a request, or legal process, is received by, or made known to, Frontier, unless disclosure of the request, or legal process, would be in violation of U.S. law, or in violation of an order of a court of competent jurisdiction in the United States.

14. Frontier agrees not to comply with such requests from Foreign Governments and Unauthorized Foreign Persons without prior written consent of USDOJ, or an order of a court of competent jurisdiction in the United States.

15. Frontier agrees to ensure that U.S. Records are not subject to mandatory destruction under any Foreign laws.

Unauthorized Access and Security Incidents

16. Frontier agrees to take all practicable measures to prevent unauthorized Access to U.S. Records, DC, and the DCI.

17. Frontier agrees to take all practicable measures to prevent any unlawful use or disclosure of information relating to U.S. Records or DC.

18. Frontier agrees to provide, upon request by USDOJ, its (1) cybersecurity plans; and (2) Network System Security Plans (“NSSP”). Frontier agrees that its cybersecurity plans will conform with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Frontier further agrees to make modifications to these plans, if requested by USDOJ, and to work with USDOJ to implement such modifications, including conferring with USDOJ with regard to any objections to such modifications.

19. Frontier agrees that its NSSPs will include, among other things, policies relating to its information security, supply chain security, remote access, physical security, cybersecurity, third-party contractors, Outsourcing and Offshoring, maintenance and retention of system logs, protection of Lawful U.S. Process, protection of U.S. Records obtained by Frontier in the ordinary course of business, and Frontier’s plans regarding new contracts or amendments to existing contracts with third-party providers requiring those third parties to notify Frontier in the event of a breach or loss of U.S. Records within a specified time period after discovery, not to exceed 48 hours from the time of discovery.

20. Frontier agrees to provide to USDOJ updated network diagrams to include all primary facilities, devices, Points of Presence (PoPs), and NOCs upon request. Frontier agrees to provide detailed information about any facilities, devices, PoPs, and NOCs upon further request.

21. Frontier agrees to notify USDOJ at least 30 days prior to changing the primary and secondary locations for storage of U.S. Records (as previously reported to the USDOJ) for

USDOJ objection or non-objection. USDOJ will object or not object to such change in location within 30 days of notification. Such notice shall include:

- a. A description of the type of information to be stored in the new location;
- b. The custodian of the information (even if such custodian is Frontier);
- c. The location where the information is to be stored;
- d. The factors considered in deciding to store that information in the new location;
and
- e. A description of the physical/logical protections at the new location.

Reporting Incidents and Breaches

22. Frontier agrees to report to USDOJ promptly, and in any event no later than 72 hours, after if it learns of information that reasonably indicates:

- a. A Security Incident, other than an immaterial (i) unplanned disruption to a service or (ii) denial of a service;
- b. Unauthorized Access to, or unauthorized disclosure of, any information relating to services provided by Frontier, or referring or relating in any way to Frontier's customers in the United States or its territories, other than immaterial inadvertent disclosures of such information by Frontier employees or Outsourced or Offshore service providers;
- c. Any unauthorized Access to, or unauthorized disclosure of, DC in violation of federal, state, or local law; or
- d. Any breach of the commitments made in this LOA.

23. Frontier agrees to require any third-party service provider in new or amended agreements to disclose to Frontier any data breach of any U.S. Records, or any loss of U.S. Records, whether from a data breach, or other cause, within 48 hours of the third party discovering the breach or loss. With respect to existing agreements, Frontier may provide notice to third-party service providers requiring disclosure.

24. Frontier agrees to notify USDOJ, including the points of contact (POC) listed in this LOA, in writing of any of the Security Incidents or breaches described in this LOA. Such notification shall take place no later than 5 days after Frontier discovers, or receives notice from any third party providing Outsourced or Offshored services of, the incident, intrusion, or breach has taken or is taking place, or sooner when required by statute or regulations.

25. Frontier agrees to notify the FBI and U.S. Secret Service as provided in 47 C.F.R. § 64.2011 within seven business days after reasonable determination that a person without authorization, or in exceeding their authorization, has gained Access to, used, or disclosed CPNI,

or that of a third party used by Frontier, and shall electronically report the matter to the central reporting facility through the following portal: <https://www.cpnireporting.gov>.

Principal Equipment

26. Frontier agrees to prepare a Principal Equipment List in a usable and searchable format. Frontier agrees to provide the USDOJ within 90 days from the Date of FCC Approval, a Principal Equipment List in a usable format for USDOJ objection or non-objection within 90 days. The Principal Equipment List shall include, to the extent determinable from Frontier's existing business records or from further investigation on a case-by-case basis as requested by USDOJ, the following:

- a. A complete and current list of all Principal Equipment in a usable format, including:
 - i. a description of each item and the functions supported,
 - ii. each item's manufacturer, and
 - iii. the model and/or version number of any hardware or software.
- b. Any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment.

27. Frontier agrees to notify USDOJ in writing at least 30 days prior to introducing any new make or model of Principal Equipment (where such make or model was not already identified to USDOJ) for USDOJ objection or non-objection. USDOJ will object or non-object to such new Principal Equipment to the Principal Equipment within 30 days of receipt of notice.

28. Frontier agrees to provide USDOJ with the names of providers, suppliers, and entities that will perform any maintenance, repair, or replacement that may result in any introduction of new Principal Equipment or modification to its Principal Equipment or systems or software used with or supporting the Principal Equipment. USDOJ will object or non-object to the nominated providers, suppliers, and entities selected by Frontier within 30 days of receipt of notice.

Outsourced and Offshored Services

29. Frontier agrees to provide the USDOJ within 90 days from the Date of FCC Approval, a list of all Outsourced or Offshored service providers that provide services described in (a)-(f) below to Frontier for USDOJ objection or non-objection.

- a. MNSP services;
- b. NOC(s);
- c. Network maintenance services;

- d. Billing or customer support services;
- e. Any operation or service that could potentially expose the DCI, Domestic Communications, or U.S. Records to include CPNI such as CDRs; and
- f. Deploying any network elements, hardware, software, core network equipment, and network management capabilities that are owned, managed, manufactured, or controlled by a Foreign Government or Foreign entities.

30. Frontier agrees to notify USDOJ in writing no less than 30 days prior to the use of any new Outsourced or Offshore service providers that will provide any of the services described in Paragraph 29(a)-(f) above.

31. USDOJ agrees to object or non-object to any new Outsourced or Offshore service providers, within 30 days of receiving notice.

Emergency Remediation

32. Where complying with Paragraphs 27, 28, or 30 would risk immediate and substantial harm to telecommunications infrastructure, systems or customer services, Frontier may undertake emergency remediation measures without first seeking the required advance USDOJ approval. Frontier must notify USDOJ as soon as practicable, but no later than 48 hours after initiating the remedial measures. Such notification must contain an explanation for proceeding without advance approval, a description of the emergency and an explanation as to why prior notification did not or could not occur. USDOJ retains the right to object to the Principal Equipment or Outsourced or Offshore Services employed or otherwise used to address the emergency, and if USDOJ objects Frontier agrees to resolve the objection to USDOJ satisfaction.

Network Operations Centers

33. Frontier agrees to seek USDOJ approval for the location of any non-U.S. NOC prior to providing services under an FCC international Section 214 authorization. If USDOJ does not approve the location of a non-U.S. NOC, Frontier agrees not to use the non-U.S. NOC.

34. Frontier agrees to notify USDOJ in writing at least 60 days prior to changing the location of its NOCs to a non-U.S. location for USDOJ objection or non-objection.

Change in Ownership and Service Portfolio

35. Frontier agrees to provide USDOJ notice of any changes to its business, including but not limited to corporate structure changes, corporate name changes, business model changes, corporate headquarter location changes, or business operation location changes no less than 30 days in advance of such change (other than changes in the location of customer premises equipment in the ordinary course of business), but notices of pro forma transactions may be provided concurrently with notice to the FCC. Frontier agrees to

provide USDOJ notice of any person or entity acquiring a sufficient ownership interest in Frontier that results in changes to stock or board voting rights or the ability to designate board members that allows for Access to Frontier's confidential business information within 30 days after becoming aware of such ownership interest. Frontier also agrees to provide USDOJ notice within 30 days of initiating any bankruptcy proceeding or any other legal proceeding undertaken for the purpose of liquidating, reorganizing, refinancing, or otherwise seeking relief from all or some of Frontier's debts.

36. Frontier agrees to provide USDOJ notice of any material change to its current portfolio of services offering, including offering other services beyond its current service portfolio, no less than 30 days in advance of such change for USDOJ objection or non-objection.

Annual Report

37. Frontier agrees to provide an annual report to USDOJ regarding the company's compliance with this LOA, to include:

- a. Certification that there were no changes during the preceding year (where no changes were reported to USDOJ during the year);
- b. Notice(s) regarding the company's handling of U.S. Records, DC, and Lawful U.S. Process (*i.e.*, whether handled properly and in accordance with the assurances contained herein) including a list of any Unauthorized Foreign Persons with Access to U.S. Records not previously reported to USDOJ;
- c. Notification(s) of the installation and/or purchase or lease of any new makes or models of Foreign-manufactured telecommunication equipment not previously reported to USDOJ (including, but not limited to, switches, routers, software, hardware);
- d. Notification(s) of any relationships with Foreign-owned telecommunications partners, including any network peering (traffic exchange) or interconnection relationships not previously reported to USDOJ;
- e. Updated Nssp and cybersecurity plan;
- f. Updated network diagrams (to include all facilities, devices, Points of Presence (PoPs), and NOCs);
- g. Report(s) of any occurrences of Security Incidents including but not limited to cyber-security incidences, network and enterprise breaches, and unauthorized access to U.S. Records;
- h. A re-identification of the location that Frontier stores U.S. Records;
- i. Recertification of the services that Frontier provides or confirmation that no additional services are being offered;

- j. Recertification that the location of all non-U.S. NOCs have been approved by USDOJ;
- k. A re-identification of the name of and contact information of the LEPOC;
- l. Certification of compliance with CALEA and any other applicable U.S. lawful interception statutes, regulations, and requirements;
- m. Notification of any reasonably foreseeable matter that would give rise to an obligation under this LOA.

The annual report will be due one year after the Date of this LOA and every year thereafter. Frontier agrees to send electronic copies of the annual report and all notices and communications required under this LOA to the following individuals or any other individuals that DOJ identifies to Frontier in the future: Alice Suh Jou, USDOJ (at alice.s.jou2@usdoj.gov); Loyaan Egal, USDOJ and Eric Johnson, USDOJ (at Compliance.Telecom@usdoj.gov). Upon USDOJ request, Frontier agrees to provide USDOJ with paper copies of any annual report, notices, or communications required under this LOA.

Site Visits

38. Frontier agrees to permit USDOJ's requests for site visits and approve all requests to conduct on-site interviews of Frontier employees to verify the implementation of and compliance with the terms of this LOA, or to identify grounds for modification of this LOA.

Miscellaneous

39. Frontier agrees to permit disclosure of confidential information submitted to the FCC pursuant to 47 C.F.R. § 0.442 to Federal government departments, agencies, and offices whose principals are listed in Exec. Order 13913 § 3.

40. If USDOJ finds that the terms of this LOA are inadequate to resolve any national security or law enforcement risks, Frontier agrees to negotiate in good faith and promptly to resolve these risks, according deference to the USDOJ's views on the need for modification. Rejection of a proposed modification shall not alone be dispositive, but failure to resolve national security or law enforcement risks may result in a recommendation that the FCC modify, condition, revoke, cancel, terminate, or render null and void any relevant license, permit, or other authorization granted by the FCC to Frontier or its successors-in-interest, or any other appropriate enforcement action required to address the risks.

41. Frontier agrees that in the event that Frontier breaches the material commitments set forth in this LOA, to include conduct contrary to timely USDOJ objection to any notice submitted pursuant to this LOA, a recommendation may be made that the FCC modify, condition, revoke, cancel, enter other declaratory relief, or render null and void any relevant license, permit, or other authorization granted by the FCC to Frontier or its successors-in-interest, in addition to pursuing any other remedy available by law or equity.

42. If Frontier believes that changed circumstances warrant terminating this LOA, USDOJ will engage in discussions with Frontier to determine whether these changed circumstances warrant termination consistent with Executive Order 13913.

43. This LOA shall be considered null and void in the event the restructuring described in the FCC Applications is not consummated.

44. For purposes of counting days in this LOA, the day of the event that triggers the period is excluded, but every day thereafter is counted, including intermediate Saturdays, Sundays, and legal holidays. Include the last day of the period, but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or legal holiday.

45. Frontier understands that, upon execution of this LOA by an authorized representative or attorney, or shortly thereafter, the FCC will be notified that there is no objection to grant of the application.

Sincerely,



Mark D. Nielsen
Executive Vice President and Chief Legal Officer
Frontier Communications Corporation, Debtor-in-
Possession