November 7, 2017

Assistant Secretary for Policy
U.S. Department of Homeland Security
Office of Policy
Foreign Investment Risk Management
3801 Nebraska Avenue NW
Washington, D.C. 20528
IP-FCC@hq.dhs.gov

Mr. Richard C. Sofield
Director, Foreign Investment Review Staff
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001
ttelecom@jmd.usdoj.gov

Department of Defense Chief Information Officer
c/o Mr. Donald Davidson, Director Implementation & Acquisition Integration
6000 Defense Pentagon, Room 3D1048
Washington, DC 20301-6000
osd.pentagon.dod-cio.list.team-telecom@mail.mil

General Counsel
c/o James DeBose, Associate General Counsel
Defense Information Systems Agency
6910 Cooper Avenue
Fort Meade, MD 20755
james.w.debose.civ@mail.mil

Ladies and Gentlemen:

This Letter of Assurances ("LOA") outlines the commitments made by Lumos Networks Corp. ("Lumos") to the U.S. Department of Homeland Security ("DHS"), the Department of Justice ("DOJ"), and the U.S. Department of Defense ("DOD"), together "the USG Parties," in order to address national security, law enforcement, and public safety concerns raised with regard to applications filed by Lumos and MTN Infrastructure Topco, Inc. with the Federal Communications Commission ("FCC") requesting authorization to transfer indirect control of certain domestic and international Section 214 authorization holders.[1]

Lumos has agreed to provide this LOA to the USG Parties to address issues raised by the USG Parties, and Lumos understands that the USG Parties will petition the FCC to condition the requested authorizations on compliance with this LOA.

[1] ITC-T/C-20170302-00027, WC Docket No. 17-60.

For purposes of this LOA the following Definitions apply:

A. "Domestic Communications" means: (a) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States. "Electronic Communication" has the meaning given it in 18 U.S.C. § 2510(12). "Wire Communication" has the meaning given it in 18 U.S.C. § 2510(1).

B. "Domestic Communications Infrastructure" or "DCI" means: (a) the transmission and switching equipment (including hardware, software, and upgrades), routers, servers, security appliances, and fiber and copper cable and associated facilities owned (to include leased) and controlled by or on behalf of Lumos to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment leased or owned by or on behalf of Lumos that are physically located in the United States; (c) the property, facilities and equipment leased or owned by or on behalf of Lumos to control the equipment or facilities described in (a) and (b) above. The phrase "on behalf of," as used in this paragraph, does not include entities with which Lumos has contracted for peering, interconnection, roaming, long distance, or other similar arrangements.

C. "Principal Equipment" means the primary electronic components of or supporting a mobile or fixed communication network, broadband network, transport or fiber network, or terrestrial wireless or satellite network (including earth stations), used by or on behalf of Lumos to provide, process, direct, control, supervise, or manage Domestic Communications.

Principal Equipment includes, but is not limited to: (a) switches (circuit-, packet-, and softswitches); (b) network routers; (c) call managers/servers; (d) network operations center ("NOC") equipment; (e) evolved packet core ("EPC") equipment and software necessary to operate and maintain a base station; (f) digital transmitters; (g) wired and wireless radio transmitters; (h) multiplexers; and (i) any firmware necessary for the proper operation of (a) - (h), with the exception of commercial off-the-shelf ("COTS") software used for common business functions from vendors approved by the USG Parties.[2]

Upon grant of the requested FCC authority, Lumos undertakes to comply with the following commitments:

[2] Lumos understands that modification of this definition may be necessary due to changes in technology or other circumstances, and agrees to cooperate in good faith with the USG Parties to effectuate any appropriate amendments to this LOA.

1. Security Officer

Within thirty (30) business days of the execution of this LOA, Lumos shall nominate a Security Officer for purposes of this LOA. The Security Officer will be an employee of Lumos, will have appropriate senior-level corporate authority within Lumos, and will have the necessary resources and skills to maintain Lumos's security policies and procedures and oversee Lumos's compliance with this LOA. The Security Officer will be a resident U.S. citizen, and, if not already in possession of a U.S. security clearance, shall be eligible to hold such security clearance immediately upon appointment. The Security Officer will be subject to the USG Parties' review and non-objection and may be subject to a background check at the sole discretion of the USG Parties. If the USG Parties object to the Security Officer nominee, such objection must be made within thirty (30) business days of receiving notice of the nominee. The Security Officer will serve as the primary point of contact for the USG Parties regarding any national security, law enforcement, or public safety concerns that the USG Parties may raise. The Security Officer shall be responsible for receiving and promptly effectuating any requests for information pursuant to this LOA and for otherwise ensuring compliance with obligations set forth in this LOA. Lumos shall notify the USG Parties of any proposed change to the Security Officer at least ten (10) business days in advance of such change where possible. Any subsequently proposed Security Officer shall be subject to the USG Parties' review and non-objection and may be subject to a background check at the sole discretion of the USG Parties. As applicable, the Security Officer will instruct and train Lumos officers, employees, contractors and agents on the requirements of this LOA.

2. Initial Principal Equipment List

Within thirty (30) business days of the execution of this LOA, Lumos shall provide the USG Parties with a list to include:

(a) A complete and current list of all Principal Equipment, including: (1) the name and a description of each item and the functions supported, (2) each item's manufacturer, and (3) the production year, model and/or version number of any hardware or software; and

(b) Any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment, including a description of the type of service offered by the vendor, contractor, or subcontractor.

The USG Parties shall approve or disapprove the Initial Principal Equipment List within thirty (30) business days of receipt, unless otherwise delayed by awaiting responses to inquiries for further information from Lumos, in which event the USG Parties shall be afforded additional time to approve or disapprove the Initial Principal Equipment List. The USG Parties' additional time to approve or disapprove shall be the original thirty (30) business day window extended by the number of days the USG Parties awaited a response from Lumos. Failure by the USG Parties to respond within the required timeframe shall be deemed to constitute a non-objection to use of

the equipment included on the Initial Principal Equipment List and the services of the vendors, contractors, or subcontractors identified on the Initial Principal Equipment List.

3. Material Modifications to Existing Principal Equipment

Lumos shall provide the USG Parties at least thirty (30) business days' advance notice prior to performing any maintenance, repair, or replacement that would result in any material modification to existing Principal Equipment. Lumos need not comply with the advance notice requirement for any maintenance, repair, or replacement that is undertaken in response to an unforeseen or uncontrollable event and that is necessary to ensure the continued operability of the Lumos network; however, in such circumstances, Lumos shall provide advance notice to the USG Parties of the material modification, if practicable, and, if impracticable, Lumos shall provide notice within ten (10) business days after the material modification of the Principal Equipment. Lumos may continue to utilize any Principal Equipment repaired or replaced pursuant to the process outlined in this paragraph, provided that the USG Parties do not object within thirty (30) business days of notification.

4. Change in Vendors, Contracts, or Subcontracts for Principal Equipment

Lumos shall provide at least thirty (30) business days' advance notice prior to making any modifications to the list of vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment. In addition, Lumos shall provide at least thirty (30) business days' advance notice prior to changing the service offerings or support from a previously-listed vendor, contractor, subcontractor (*i.e.*, where a previously-listed provider will be offering support in a previously unidentified way). The USG Parties shall approve or disapprove any modification or change proposed pursuant to this paragraph within thirty (30) business days of receipt, unless otherwise delayed by awaiting responses to inquiries for further information from Lumos, in which event the USG Parties shall be afforded additional time to approve or disapprove the proposed modification or change. The USG Parties' additional time to approve or disapprove shall be the original thirty (30) business day window extended by the number of days the USG Parties awaited a response from Lumos. Failure by the USG Parties to respond within the required timeframe shall be deemed to constitute a non-objection to proposed modification or change.

5. Measures to Prevent Improper Use and Unauthorized Access

Lumos agrees to take all reasonable measures to prevent unauthorized access to the DCI and to prevent any unlawful use or disclosure of information carried on the same. Such measures shall include a National Institute of Standards and Technology (NIST) -compliant cyber-security plan, security procedures for any remote virtual private network ("VPN") access to the DCI, contractual safeguards and screening procedures for personnel with administrative access to the DCI; and procedures for applying security patches to systems and applications. Lumos will submit policies regarding logical security measures for the DCI to the USG Parties within sixty (60) business days of the date of execution of this LOA. Lumos agrees to meet and confer with the USG Parties regarding such policies upon request.

6. Physical Security Measures

Lumos agrees to take all reasonable measures to physically secure the DCI, including by performing background screening on appropriate personnel. Lumos will screen appropriate personnel, require that all visitors who physically access the DCI are escorted at all times by screened personnel, and maintain a visitor log that will be made available to the USG Parties upon request. Lumos's personnel screening process shall be reflected in a written policy and will include background investigations, public criminal records checks, or other analogous means to ascertain a person's trustworthiness. In addition, Lumos will cooperate with any reasonable notice by the USG Parties to provide additional information necessary for an enhanced background investigation to be conducted by the USG Parties with respect to personnel with access to the DCI. Lumos will submit policies regarding physical security measures for the DCI to the USG Parties within sixty (60) business days of the date of execution of this LOA. Lumos agrees to meet and confer with the USG Parties and to consider any concerns the USG Parties may raise about Lumos's physical security measures.

7. Physical and Information Access List

Within thirty (30) business days of the execution of this LOA, Lumos shall provide the Department of Justice with a list of:

(a) All persons who have Access to Classified Information;

(b) All persons who have access to Sensitive Information;

(c) All persons who have Access to Domestic Communications Infrastructure to monitor the content of Domestic Communications;

(d) All persons who have the ability to monitor personnel with limited access to Domestic Communications under this subsection;

(e) All persons who have Access to Transactional Data, Subscriber Information, CPNI, CDRs, IPDRs, or PII for customers and network users of Lumos;

(f) All persons who have limited access to Domestic Communications Infrastructure;

(g) All persons who provision network elements either onsite or remotely:

(h) All vendors, contractors, or subcontractors, including billing vendors and managed service providers, involved in Accessing, managing, or maintaining CDR, Classified Information, CPNI, IPDR, PII, Sensitive Information, Subscriber Information or Transactional Data; and

(i) All vendors, contractors, or subcontractors, including managed service providers, involved in providing network or software services, to include network security and cloud solutions.

The Department of Justice shall approve or disapprove any person included on the list required pursuant to this paragraph within thirty (30) business days of receipt unless extended or otherwise delayed by awaiting responses to inquiries for further information from Lumos, in which event the Department of Justice shall be afforded additional time to approve or disapprove the listed person. The Department of Justice's additional time to approve or disapprove shall be the original thirty (30) business day window extended by the number of days the Department of Justice awaited a response from Lumos. Failure by the USG Parties to respond within the required timeframe shall be deemed to constitute a non-objection to the listed person.

Lumos shall provide the Department of Justice at least thirty (30) business days' advance notice prior to making any modifications to the list of vendors, contractors, or subcontractors, including but not limited to billing vendors and managed service providers, involved in Accessing, managing, or maintaining CDR, Classified Information, CPNI, IPDR, PII, Sensitive Information, Subscriber Information or Transactional Data. In addition, Lumos shall provide at least thirty (30) business days' advance notice prior to changing the service offerings or support from a previously-listed vendor, contractor, subcontractor, including billing vendors and managed service providers, involved in Accessing, managing or maintaining CDR, Classified Information, CPNI, IPDR, PII, Sensitive Information, Subscriber Information or Transactional Data (*i.e.*, where a previously-listed provider will be offering support in a previously unidentified way). Furthermore, Lumos shall provide the Department of Justice at least thirty (30) business days advance notice prior to making any modifications to the list of managed service providers or changing the service offerings or support from a previously-listed managed service provider. The Department of Justice shall approve or disapprove any modification or change proposed pursuant to this paragraph within thirty (30) business days of receipt unless extended or otherwise delayed by awaiting responses to inquiries for further information from Lumos.

Notwithstanding the foregoing, in the event of exigent circumstances, the Department of Justice may extend the time for its approval or disapproval of any notice provided by Lumos under this Section 7 by a maximum of thirty (30) additional business days, by giving written notice of such extension to Lumos within thirty (30) business days of the initial receipt of the notice. The Department of Justice agrees that it will make good-faith efforts to respond to each notice within the initial thirty (30) business day period (subject to any automatic extensions provided for above) and will not routinely request extensions under this paragraph.

For purposes of this Section 7 only, the following definitions apply:

A. "Access" or "Accessible" means the ability to physically or logically undertake any of the following actions:
    I. read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system, or a network;

II. read, edit, or otherwise obtain non-public information regarding internal Lumos personnel, contractors, service partners, subscribers, or users;
III. add, edit, or alter information or technology stored on or by software, hardware, a system, or a network; and
IV. alter the physical or logical state of software, hardware, a system, or a network (e.g., turning it on or off, changing configuration, removing or adding components or connections, etc.).

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. "Classified Information" means any information determined pursuant to Executive Order 13,526, as amended or superseded, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.

D. "Customer Proprietary Network Information ("CPNI") means:

I. information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship;
II. information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information; and/or
III. information falling within the definition given in 47 U.S.C. § 222(h)(1).

E. "Internet Protocol Detail Record" ("IPDR") means a streaming data protocol used by Operations Support Systems ("OSS") and Business Support Systems ("BSS") to collect and record a user's data traffic statistics on a network.[3]

F. "Personal Identifiable Information" ("PII") means the name and aliases, social security number, date of birth, place of birth, citizenship status, contact information, and current address of an individual.

G. "Sensitive Information" means information that is not Classified Information regarding:

I. the persons or facilities that are the subjects of lawful U.S. process;
II. the identity of the government agency or agencies serving such lawful U.S. process;

[3] IPDR mainly is used by cable industries and incorporated into Cablelabs Data Over Cable Service Interface Specification ("DOCSIS") protocol. DOCSIS is a standard interface for cable modems. It provides network usage and user information for network management.

III. the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct electronic surveillance;
IV. the means of carrying out electronic surveillance;
V. the type(s) of service, telephone number(s), records, communications, or facilities subjected to lawful U.S. process; and
VI. other information that is not Classified Information designated in writing by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information."

H. "Subscriber Information" means information of the type referred to and accessible subject to the procedures specified in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

I. "Transactional Data" means:

I. any "call identifying information," as defined in 47 U.S.C. § 1001(2), as amended or superseded, including, without limitation, the telephone number or similar identifying designator associated with a communication;[4]
II. Internet address or similar identifying designator associated with a communication;
III. the time, date, size, and duration of a communication;
IV. any information relating specifically to the identity and physical/logical address of a subscriber, user, or account payer of Lumos;
V. to the extent associated with a subscriber, user, or account payer of Lumos, any information relating to telephone numbers, Internet addresses, e-mail accounts, text messages, Instant Messages ("IMs") or similar identifying designators, to include the physical location of equipment, if known and if different from the location information provided under (f), below, and the types of service, length of service, fees, and usage, including CDRs, CPNI, and any other billing records; and
VI. any information indicating, as closely as possible, the physical location to or from which a communication is transmitted.

8. Reporting Incidents and Breaches

Lumos agrees to report to the USG Parties promptly if it learns of information that reasonably indicates:

(a) Unauthorized third-party access to, or disruption or corruption of, the DCI or any information being carried on the DCI;

(b) unauthorized or improper access to or disclosure of Domestic Communications in violation of U.S. law; or

[4] Also includes Uniform Resource Locators ("URLs") and Internet Protocol ("IP") address/header information.

(c) any material breach of the commitments made in this LOA.

Any reports required by this provision should be made in writing to the USG Parties within ten (10) business days of the reasonable determination by Lumos that an incident is reportable under this section. Lumos further agrees to cooperate with the USG Parties' recommendations with respect to the remediation of such events and, to the extent such recommendations are not adopted by Lumos, to provide an explanation as to why such measures are not adopted. Lumos will provide this explanation, as well as a description of any other actions taken in response to a remediation recommendation from the USG Parties, within ten (10) business days of receipt of such recommendation.

9. Instruction of Obligations

Lumos shall instruct and train appropriate officials, employees, contractors, and agents as to Lumos's obligations under this LOA, including the individuals' duty to report any violation, and shall issue periodic reminders of such obligations. Lumos shall issue these instructions in writing within sixty (60) business days of the date of execution of this LOA. Lumos will submit a copy to the USG Parties at the same time. Upon request, Lumos agrees to provide the USG Parties a listing of employees who have completed LOA training.

10. USG Customer Data

Consistent with contractual requirements, Lumos agrees not to monitor, collect, market, or sell data from any U.S. Government customers in any way, including for any commercial purpose. This is not intended to conflict with any law enforcement provision of this LOA or other legal requirements.

11. Annual Report

On or before each anniversary of the date of execution of this LOA, Lumos will submit to the USG Parties a report assessing Lumos's compliance with the terms of this LOA for the preceding year. The report shall include:

(a) The name and contact information of the Security Officer;

(b) An updated Principal Equipment List, as set forth in Section 2 above;

(c) A copy of the then-current policies adopted in accordance with this LOA and a summary of any changes during the reporting period and the reasons therefore;

(d) A summary of any events that occurred during the reporting period that will or reasonably could impact the effectiveness of or compliance with this LOA; and

(e) A summary of any known acts of noncompliance with the terms of this LOA that occurred during the reporting period, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future.

12. USG Parties Consultation and Visitation

Lumos agrees to meet and confer with the USG Parties and to address any concerns the USG Parties may raise about materials submitted pursuant to this LOA.

Lumos agrees to negotiate in good faith to resolve any national security, law enforcement, or public safety concerns the USG Parties may raise with respect to any matters set forth in this LOA.

Lumos agrees that, upon reasonable advance notice, the USG Parties may visit any part of the DCI to conduct on-site reviews concerning the implementation of the terms of this LOA and Lumos' compliance with its terms. Subject to applicable law, during such visits, Lumos shall cooperate with the requests of the USG Parties to make available information, facilities, and personnel to verify compliance with the terms of this LOA.

This LOA shall inure to the benefit of, and shall be binding upon, Lumos and its successors, assigns, subsidiaries, and affiliates.

Lumos agrees that, in the event the commitments set forth in this letter are breached, in addition to any other remedy available at law or equity, the USG Parties may request 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 Lumos or any successors-in-interest.

Lumos understands that, promptly upon execution of this letter by an authorized representative or attorney for Lumos, the USG Parties shall notify the FCC that it has no objection to the FCC's grant of the pending application.

For and on behalf of Lumos Networks Corp.

Timothy G. Biltz
Chief Executive Officer