



1120 South Tryon St.
Suite 700
Charlotte, NC 28203
brightspeed.com

July 19, 2022

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

Office of Foreign Investment Review, Director
Undersecretary of Acquisition and Sustainment
U.S. Department of Defense
1400 Defense Pentagon
Washington, DC 20301
osd.pentagon.ousd-a-s.list.team-telecom@mail.mil

Subject: WC Docket 21-350, ITC-T/C-20210903-00139, ISP-PDR-20211028-00008; TT
21-083 to -085

Applications by Connect Holding, LLC, Lumen Technologies, Inc., and certain affiliates for consent to transfer of control of authority pursuant to Section 214 of the Communications Act of 1934, as amended, to provide global or limited global facilities-based and global or limited global resale services; and
Petition for Declaratory Ruling by Consolidated Communications, Inc. asking the Federal Communications Commission to find that it would serve the public interest to approve the increase of direct or indirect foreign equity and voting interests in Connect Holding LLC, pursuant to Section 310(b)(4) of the Communications Act of 1934, as amended, 47 U.S.C. § 310(b)(4), and Section 1.5000(a)(1) of the Commission's rules, 47 C.F.R. § 1.5000(a)(1).

Dear Sirs:

This Letter of Agreement (“LOA” or “Agreement”) sets forth the commitments that Connect Holding, LLC and AP (Connect) VoteCo, LLC (“VoteCo”) (together, the “New Owners”) make to the U.S. Department of Justice (“USDOJ”), including the Federal Bureau of Investigation (“FBI”) and the U.S. Department of Defense (“USDOD,” and together with USDOJ, the “Compliance Monitoring Agencies” or “CMAs”), to address national security and



law enforcement risks arising from the above-referenced applications to the Federal Communications Commission (“FCC” or the “Commission”) requesting: (1) consent to transfer control of authorizations to provide domestic facilities-based and resale telecommunications services, pursuant to Section 214 of the Communications Act of 1934, as amended (the “Act”), 47 U.S.C. § 214, and the implementing regulation at 47 C.F.R. § 63.04; (2) consent to transfer control of an authorization to provide global or limited global resale services between the United States and permissible international points pursuant to Section 214 of the Act, and the implementing regulation at 47 C.F.R. § 63.18(e)(2);¹ (3) consent to transfer control of wireless licenses pursuant to Section 310(d) of the Act, 47 U.S.C. § 310(d);² and (4) FCC approval of an increase in the direct and indirect foreign equity and voting interests in Connect, pursuant to Section 310(b)(4) of the Act and Section 1.5000(a)(1) of the Commission’s rules.³

The applications described above relate to a pending transaction (the “Transaction”) involving Connect Holding, LLC’s indirect acquisition of certain affiliates of Lumen Technologies, Inc. (“Lumen”). Those Lumen affiliates (the “Transferred Business”) hold the authorizations that are the subject of the above-noted applications. As used in this LOA, the term “Connect” refers to Connect Holding, LLC and all of its current and future direct and indirect subsidiaries, including (when and if the Transaction closes) the entities comprising the Transferred Business.

Connect certifies as true and correct, under penalties outlined in 18 U.S.C. § 1001, all statements it or its representatives have made to USDOJ, the Department of Homeland Security, USDOD, and the FCC in the course of the review of the above-referenced application that was conducted pursuant to Executive Order 13913,⁴ and hereby adopt 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,

¹ ITC-214-20000706-00385.

² See FCC File Numbers 0009669963 (lead call sign WQR37); 0009669967 (lead call sign WLC623); 0009669970 (lead call sign WFY653); 0009669971 (lead call sign KNKG844); 0009669972 (lead call sign WQLJ485); 0009669973 (lead call sign KNKG811); 0009669974 (lead call sign KNKP350) 0009669977 (lead call sign WQMN435); 0009669980 (lead call sign KYO87); 0009669985 (lead call sign KJH26).

³ See ISP-PDR-20211028-00008.

⁴ 85 Fed. Reg. 19643 (Apr. 8, 2020).



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 a 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. “Cybersecurity Incident Response Plan” means a plan or processes put in place to develop and implement the appropriate activities to take action regarding a detected cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

e. “Date of FCC Approval” means the date on which the FCC releases a public notice granting the FCC Application.

f. “Domestic Communications” (“DC”) means:

- (i) Wire Communications or Electronic Communications, as defined by 18 U.S.C. § 2510, (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 any Connect 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 of, Connect to provide, process, direct, control, supervise, or manage DC but would not include the systems of entities for which Connect has a contracted arrangement for interconnection, peering, roaming, long-distance, or wholesale network Access.

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. “Geolocation Data” means any information collected by Connect from its customers regarding a customer’s location or the customer’s device location.
- k. “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.
- l. “Internet Protocol Detail Record” (“IPDR”) means information about internet protocol-based usage and other activities that can be used by operation support systems (“OSS”) and business support systems (“BSS”) by recording data statistics that provide network insight on capacity, subscriber usage, and proactive network maintenance.
- m. “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.

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

- (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; OSS; BSS; Network Operations Centers (“NOCs”); information technology; cloud operations/services; 5G (Software Defined Networking, Network Functions Virtualization, Applications); and datacenter services and operations.

o. “Network Operations Center” (“NOC”) means any locations and facilities performing network management, monitoring, accumulating accounting and usage data, maintenance, user support, or other operational functions for DC.

p. “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 Connect.

q. “Outsource” means, with respect to DC, supporting the services and operational needs of Connect at issue in this LOA using contractors or third parties.

r. “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.

s. “Principal Equipment” means all telecommunications and information network equipment (*e.g.*, hardware, software, platforms, operating systems, applications, protocols) that supports core telecommunications or information services, functions, or operations.



t. “Security” means a condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization’s risk management approach.

u. “Security Incident” means:

- (i) Any known or suspected breach of this LOA, including a violation of any approved plan, policy, or procedure under this LOA;
- (ii) Any unauthorized Access to, or disclosure of, U.S. Records;
- (iii) Any unauthorized Access to, or disclosure of, information obtained from or relating to Government entities; or
- (iv) Any one or more of the following which affect the company’s computer network(s) or associated information systems:
 - A. Unauthorized 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, including the identification of vulnerabilities introduced through a cyber supply chain compromise;
 - D. Unplanned incidents that cause activation of Connect’s Cybersecurity Incident Response Plan;
 - E. Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect the company’s ability to comply with the terms of this LOA; or
 - F. An unauthorized occurrence that (1) actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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

w. “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.



x. “U.S. Records” means Connect’s customer billing records, Subscriber Information, PII, Sensitive Personal Data, CDRs, IPDRs, CPNI, Geolocation Data, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by Connect 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. Connect 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 the CMAs, including the FBI. The LEPOC shall be a U.S. citizen residing in the United States or its territories unless the CMAs otherwise agree in writing. The LEPOC must be approved by the FBI to receive service of Lawful U.S. Process including for U.S. Records, and, where possible, to assist and support lawful requests for Electronic Surveillance or production of U.S. Records by U.S. federal, state, and local law enforcement agencies.

3. Connect agrees to provide the LEPOC’s PII to the CMAs within 15 days of the Date of FCC Approval. The CMAs agree to object or non-object within 15 days from receiving the LEPOC’s PII.

4. Connect agrees to notify the CMAs, including the FBI, in writing at least 30 days prior to modifying its LEPOC for objection or non-objection by the CMAs. For those cases involving the unexpected firing, resignation, or death of the LEPOC, written notice will be provided within five days of such event. Under these circumstances, the CMAs will object or non-object to the replacement LEPOC within 30 days of notification.

5. Connect 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 promptly and, in any event, will respond to the request no later than five days after receiving such Lawful U.S. Process unless the CMAs grants an extension.

6. Connect agrees to implement, either directly or through a vendor, a process to screen individuals with Access to DC, DCI, or U.S. Records. Such a process shall apply to (1) Connect personnel; or (2) any personnel of an approved Outsourced or Offshored service provider performing under an agreement with Connect. The personnel screening process shall include background investigations, public criminal records checks, or other analogous means to ascertain a person’s trustworthiness. Connect further agrees to provide the CMAs with a written description of this personnel-screening process no later than 60 days after the Date of FCC Approval. The CMAs agree to object or non-object within 60 days of receiving such description. To the extent that any Connect personnel were previously subject to such screening pursuant to



Lumen policies and procedures, Connect shall: (1) identify such individuals to the CMAs; and (2) identify when they were screened pursuant to Lumen policies and procedures. The CMAs may require any such individuals to be re-screened pursuant to Connect's process if in the reasonable exercise of their discretion they believe re-screening is necessary or advisable to safeguard DC, DCI, or U.S. Records.

7. Connect agrees to notify the CMAs of all Foreign persons (e.g., Foreign employees, Foreign employees of Connect Foreign subsidiaries, and Foreign employees of approved Outsourced or Offshored service providers), that it intends to allow Access to U.S. Records, DC, or DCI. Connect agrees to make such notification no less than 30 days prior to the date by which it is seeking such Access be granted; or, with respect to any Foreign persons with such Access as of the Date of FCC Approval, within 30 days of the Date of FCC Approval. Connect further agrees to provide the PII to the CMAs for each Foreign person so identified. The CMAs agree to object or non-object within 30 days of receiving notice.

Security Officer

8. Connect agrees to designate and maintain a security officer ("Security Officer") who is a non-dual United States citizen residing in the United States and may also designate and maintain one or more alternate security officers ("Alternate Security Officer") to fulfill the responsibilities of the Security Officer in the event of his or her unavailability. The proposed Security Officer (and any Alternate Security Officer) must be eligible to obtain and maintain a "Secret" level or higher U.S. Government security clearance immediately upon appointment. The Security Officer and any Alternate Security Officer will have the appropriate authority and skills to implement the terms of this LOA and to address security concerns identified by the CMAs. The Security Officer and any Alternate Security Officer will have the appropriate senior-level corporate authority within Connect to perform his/her duties under this LOA. The Security Officer and any Alternate Security Officer will possess the necessary resources and skills to enforce this LOA and to act as a liaison to the CMAs regarding compliance with this LOA and to address any national security or law enforcement issues arising during Connect's due course of business. Connect will provide the Security Officer and any Alternate Security Officer with Access to Connect's business information that is necessary for the Security Officer and any Alternate Security Officer to perform their duties.

9. The Security Officer will be available 24 hours per day, 7 days per week, to respond to and address any national security or law enforcement concerns that the CMAs may raise with respect to Connect or its operations, except that if Connect designates an Alternate Security Officer, then in the event that the Security Officer is unavailable, the Alternate Security Officer will be available to respond to and address such concerns. Upon request by the CMAs, the Security Officer or, as applicable, Alternate Security Officer, will make himself/herself available in person within the United States or its territories within 72-hours, at a date and location, including in a classified setting, as deemed necessary by the CMAs.



10. Connect agrees to nominate a proposed candidate for Security Officer to the CMAs within 15 days of the Date of FCC Approval, and thereafter will provide at least 10 days' notice of a Security Officer's departure, and 30 days' prior notice of a new Security Officer designation (except in the case of the unexpected firing, resignation, or death of the Security Officer in which case such written notice of such departure or designation must be provided within five days of such event). Connect further agrees to not maintain a vacancy or suspension of the Security Officer position for a period of more than 60 days. In the event that Connect designates an Alternate Security Officer, Connect will nominate a proposed candidate for Alternate Security Officer at least 30 days prior to the date on which the Connect proposes to designate an Alternate Security Officer. Connect agrees to provide the proposed Security Officer's (and any Alternate Security Officer's) PII with the nomination. All Security Officer nominations and any Alternate Security Officer nominations will be subject to review and non-objection by the CMAs and may be subject to a background check at the sole discretion of the CMAs. The CMAs will object or non-object to the proposed Security Officer or Alternate Security Officer, if applicable, within 30 days of notification. Connect agrees to address concerns raised by the CMAs regarding the selection and identity of the Security Officer and any Alternate Security Officer.

Lawful U.S. Process and Requests for Information

11. Connect agrees to comply with all applicable lawful interception statutes, regulations, and requirements, as well as comply with all court orders and other Lawful U.S. Process for lawfully authorized Electronic Surveillance. Connect further agrees to certify to the CMAs 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.

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

13. Upon receipt of any Lawful U.S. Process, Connect 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 information to the requesting officials, in a manner and time consistent with the Lawful U.S. Process.

14. Connect agrees not to provide, or otherwise allow the disclosure of, or Access to, U.S. Records, DCI, or DC, to any Foreign Government, Foreign entity, or any Foreign person (other than those that (1) have been reviewed and not objected to consistent with Paragraph 7 of this LOA; or (2) are an Outsourced or Offshored service provider, or an employee thereof,



approved pursuant to Paragraphs 33-35 of this LOA), without prior written consent of the CMAs, or a court of competent jurisdiction in the United States.

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

16. Connect agrees to refer any requests for information described in Paragraphs 11 or 12 from a Foreign person (other than those that (1) have been reviewed and not objected to consistent with Paragraph 7 of this LOA; or (2) are an Outsourced or Offshored service provider, or an employee thereof, approved pursuant to Paragraphs 33-35 of this LOA) or a Foreign Government, including any legal process from a Foreign Government, to the CMAs 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, Connect, 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.

17. Connect agrees not to comply with such requests from Foreign Governments and Foreign persons without prior written consent of the CMAs, or an order of a court of competent jurisdiction in the United States.

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

Unauthorized Access and Security Incidents

19. Connect agrees to take all appropriate measures to prevent unauthorized Access to U.S. Records, DC, and the DCI.

20. Connect agrees to take all appropriate measures to prevent any unlawful use or disclosure of information relating to U.S. Records or DC.

21. Connect agrees to prepare: (1) a Cybersecurity Plan; and (2) a comprehensive System Security Plan (“SSP”) (together the “Plans”), each of which shall be guided by the current version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and incorporate applicable controls found in NIST SP 800-53, NIST SP 800-171, or other international information security standards. Connect will provide copies of those Plans to the CMAs within 60 days of the Date of FCC Approval for objection or non-objection. Furthermore, Connect agrees that the Plans will be updated when appropriate to conform with evolving information security standards, and that Connect will make additional



modifications to these Plans, if requested by the CMAs, and to work with the CMAs to implement such modifications. The CMAs agree to object or non-object within 60 days of receiving each version of the Plan.

22. Connect agrees that its Plans will include, among other things, policies relating to its information security, supply chain security, cybersecurity incident response, 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 Connect in the ordinary course of business, and Connect's plans regarding new contracts or amendments to existing contracts with third-party service providers requiring those third parties to: a) notify Connect when required under Paragraphs 25 and 26, and b) screen personnel as required under Paragraph 6.

23. Connect further agrees to take timely and appropriate remedial measures, as recommended by the U.S.-Computer Emergency Readiness Team/Cybersecurity and Infrastructure Security Agency ("US-CERT"/"CISA"), an Information Sharing and Analysis Center ("ISAC"), or other authority, to respond to and recover from any cyber or supply chain incident and mitigate vulnerabilities.

24. Connect agrees to notify the CMAs at least 30 days prior to changing the location for storage of U.S. Records or DC. The CMAs will object or non-object within 60 days of receipt of Connect's submission. 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 Connect);
- c. The location where the information is to be stored;
- d. Updated SSP and Cybersecurity Plans detailing the physical/logical protections at the new location; and
- e. The factors considered in deciding to store that information in the new location.

To the extent that the Transferred Business currently holds any U.S. Records in a location outside of the United States, Connect agrees to submit the non-U.S. location to the CMAs within 30 days of the Date of FCC Approval. The CMAs will object or non-object within 60 days of receipt of Connect's submission.

Reporting Incidents and Breaches

25. Connect agrees to report to the CMAs promptly, and in any event no later than 48 hours, after it learns of information that reasonably indicates a known or suspected:

- a. Security Incident;



- b. Unauthorized Access to, or disclosure of, any information relating to services provided by Connect, or referring or relating in any way to Connect's customers in the United States or its territories;
- c. Any unauthorized Access to, or disclosure of, DC in violation of federal, state, or local law; or
- d. Any material breach of the commitments made in this LOA.

26. Connect agrees to require any third-party service provider to disclose to Connect any data breach of any U.S. Records or DC, or any loss of U.S. Records or DC, whether from a data breach, or other cause, within 48 hours of the third party discovering the breach or loss. Connect agrees further to require any third-party service provider to disclose to Connect, within 48 hours of discovery, any critical exposure, threats, and vulnerabilities associated with the products or services provided to Connect that are the result of the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software and hardware into such products or services or into the third-party providers' supply chain. Connect may seek a permission from the CMAs to waive all or part of this paragraph for individual service providers. Such requests shall be made in writing. If a third-party service provider fails to agree to disclose such a breach, Connect shall notify the CMAs within 72 hours.

27. Connect agrees to notify the CMAs, including the points of contact ("POCs") 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 48 hours after Connect has knowledge of, or is informed by, a third party providing Outsourced or Offshored services to Connect, that the incident, intrusion, or breach has taken or is taking place, or sooner when required by statute or regulations.

28. Connect 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 his or her authorization, has gained Access to, used, or disclosed CPNI, whether through Connect's network or that of a third party used by Connect, and shall electronically report the matter to the central reporting facility through the following portal: <https://www.cpnireporting.gov>

Principal Equipment

29. Connect agrees to provide the CMAs within 30 days of the Date of FCC Approval, a Principal Equipment list. The CMAs will object or non-object to the Principal Equipment list within 60 days of receipt. The Principal Equipment list shall include the following:

- a. A complete and current list of all Principal Equipment, 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. The name, address, phone number, and website for any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment.
30. Connect agrees to notify the CMAs in writing at least 30 days prior to introducing any new Principal Equipment of a different make or model than the Principal Equipment identified and approved pursuant to Paragraph 28, or subsequently approved by the CMAs pursuant to this paragraph, or modifying any of its Principal Equipment. The CMAs will object or non-object to such new Principal Equipment or modification to the Principal Equipment within 30 days of receipt of notice.
31. Connect agrees to provide the CMAs with the name, address, phone number, and website of any 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, systems, or software used with or supporting the Principal Equipment. The CMAs will object or non-object to the nominated providers, suppliers, and entities selected by Connect within 30 days of receipt of notice.
32. Connect agrees to provide to the CMAs updated network diagrams and topology maps showing all facilities, devices, interfaces, Points of Presence ("PoPs"), exchange points, and NOCs within 60 days from the Date of FCC Approval.

Outsourced and Offshored Services

33. Connect agrees to provide the CMAs within 30 days of the Date of FCC Approval, a list of all Outsourced or Offshored service providers that provide services to Connect. The CMAs will object or non-object to the Outsourced and Offshored service provider list within 60 days of receiving notice. The list should include any Outsourced or Offshored service provider that provides services for:
- 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 DCI, DC, or U.S. Records; 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 non-public entities.



Connect further agrees to provide the name, address, phone number, website, and description of services provided for each Outsourced or Offshored service provider included on the list submitted to the CMAs pursuant to this paragraph.

34. Connect agrees to notify the CMAs in writing no less than 30 days prior to the use of any new Outsourced or Offshored service providers that will provide any of the services described in Paragraph 33. Connect further agrees to notify the CMAs in writing no less than 30 days prior to changing the services it receives from any existing Outsourced or Offshored service provider, if such change includes any of the services described in Paragraph 33. Connect agrees that such notification shall include all of the identifying information contained in Paragraph 31 for the new Outsourced and Offshored service provider.

35. The CMAs will object or non-object to any new Outsourced or Offshored service providers within 30 days of receiving notice.

Network Operations Centers

36. Connect agrees to notify the CMAs in writing at least 60 days prior to changing the location of its NOCs. DOJ will object or non-object to any new NOC location within 60 days of receiving notice of the proposed location change. Connect will provide the address, owner (even if Connect), Principal Equipment, and MNSP(s) (as well as any new Outsourced or Offshored service providers) of the NOC with the notification, as well as appropriately updated SSP and Cybersecurity Plans.

Change in Ownership and Service Portfolio

37. Connect agrees to provide the CMAs notice of any changes to its business, including but not limited to corporate structure changes, ownership changes,⁵ 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. The New Owners also agree to provide the CMAs notice within 30 days of the initiation of 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 New Owners' debts.

38. Connect agrees to provide the CMAs notice of any material change to its current portfolio of services offerings or that of the Transferred Business, including offering other

⁵ For the purposes of this paragraph, "ownership changes" means any of the following: (1) a replacement or change in control of VoteCo or any successor in its role as general partner, managing member, or other similar managing fiduciary of AP IX Connect Co-Invest Holdings, L.P., OIF II Connect Holdings, L.P., and AP IX Connect Holdings, L.P. or similar vehicles and accounts (including successors) that invest, directly or indirectly, into Connect (the "Apollo Funds"); (2) any new investment by, or change in existing rights of, any limited partner associated with any of the Apollo Funds that results in VoteCo (or its successor) giving that limited partner a right to: (a) manage or control the activities of Connect and/or any entity or asset of the Transferred Business; and/or (b) gain Access to DC, DCI, or U.S. Records. In



services beyond the current service portfolios, no less than 30 days in advance of such change. the CMAs will object or non-object within 30 days of receiving notice.

Annual Report

39. Connect agrees to provide an annual report to the CMAs regarding the company's compliance with this LOA, to include:

- a. If Connect submitted no notifications to the CMAs pursuant to this LOA during the preceding year, a certification that there were no developments that Connect was required to report under the LOA 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 individuals with Access to U.S. Records, DC, and DCI;
- c. Notification(s) of the installation, purchase, and/or lease of any Foreign-manufactured Principal Equipment;
- d. Notification(s) regarding Offshored and/or Outsourced service providers.
- e. Notification(s) of any relationships with Foreign-owned telecommunications partners, including any network peering (traffic exchange) or interconnection relationships;
- f. Updated network diagrams and topology maps showing all facilities, devices, interfaces, PoPs, exchange points, and NOCs,
- g. Updated SSP and Cybersecurity Plans;
- h. Updated organizational chart showing all owners with a five percent or greater ownership share;
- i. Report(s) of any Security Incidents;
- j. A re-identification of the location where Connect stores U.S. Records and the types of U.S. Records collected and stored;
- k. A re-identification of the name of and contact information of the LEPOC;
- l. Notification of all filings or notices to the FCC in the prior year, and a copy of these filings if requested by the CMAs;
- m. Certification of compliance with CALEA and any other applicable U.S. lawful interception statutes, regulations, and requirements;
- n. A description of the services that Connect provides in the United States to include: the specific services provided using FCC license or authorization and

addition, with respect to any calendar month during which any non-U.S. ultimate beneficial owner has acquired a direct or indirect equity interest in Connect or its subsidiaries (including, but not limited to, Connect Holding II LLC and the entities within the Transferred Business), Connect shall provide an updated list of all non-U.S. ultimate beneficial owners holding or controlling a direct or indirect equity stake (voting or non-voting) of five percent or more in the relevant entity no later than the end of the following calendar month.



- other services it provides in the United States that do not require FCC license or authorization. Such a description should also detail any services provided to government or critical infrastructure customers; and
- o. 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 FCC Approval and every year thereafter. Connect 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 the CMAs identifies to Connect in the future: Mark Goldberg, USDOJ (Mark.Goldberg@usdoj.gov); Eric Johnson, USDOJ (at Compliance.Telecom@usdoj.gov), and USDOD (osd.pentagon.ousd-a-s.list.team-telecom@mail.mil). Upon request from the CMAs, Connect agrees to provide the CMAs with paper copies of any annual report, notices, or communications required under this LOA.

Site Visits

40. Connect agrees to permit CMA requests for site visits and information, approve all requests to conduct on-site interviews of Connect employees, and provide all documents, in each case as necessary to verify the implementation of and compliance with the terms of this LOA, or to identify grounds for modification of this LOA.

Compliance Audit

41. At their sole discretion, but no more frequently than once every calendar year, the CMAs may request that Connect undergo a neutral third-party compliance audit of LOA compliance (including any plan, policy, or procedure approved under this LOA) (a “Compliance Audit”). The first Compliance Audit shall begin not earlier than two years after the Transaction closes. In connection with any Compliance Audit:

- a. Connect agrees to designate an auditor that is mutually acceptable to the CMAs and Connect. Connect agrees to nominate a compliance auditor at least 120 days before the due date of the Compliance Audit report. The CMAs will object or non-object within 30 days of the nomination.
- b. Connect will be solely responsible for any of its costs and those of the auditor associated with any Compliance Audit. The CMAs will seek to avoid the imposition of unreasonable costs on Connect when exercising their rights under this Section.
- c. The CMAs shall be consulted on the terms and scope of the review engagement and the review standards to be applied, and Connect will submit its proposed scope of work (“SOW”) agreement with the auditor within 15 days of the CMAs’



non-objection to the auditor for CMA approval or non-approval. The CMAs agree to consult with Connect regarding the topics to be covered by the SOW. The SOW shall allow for direct communication between the CMAs and the auditor, without notice to or participation of Connect.

- d. Unless otherwise agreed to by the CMAs, the Compliance Audit report shall be submitted to the CMAs by the auditor at the same time it is submitted to Connect, on or before the due date for the Compliance Audit report required by this LOA.

General Provisions

42. If the CMAs finds that the terms of this LOA are inadequate to resolve any national security or law enforcement risks, Connect agrees to resolve the CMAs' concerns, according deference to the CMAs' 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 concerns may result in a 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 Connect or its successors-in-interest, or any other appropriate enforcement action required to address the concern. Connect may seek permission from the CMAs to waive or modify any part of this LOA that becomes unnecessary or unduly burdensome. Such requests shall be made in writing.

43. New Owners agree that in the event that either of them breach the commitments set forth in this LOA, to include conduct contrary to timely CMA 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 Connect or its successors-in-interest, in addition to pursuing any other remedy available by law or equity.

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

46. Connect 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.

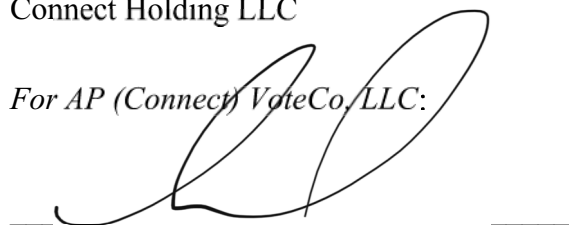


For Connect Holding LLC:



Thomas Maguire, Chief Operating Officer
Connect Holding LLC

For AP (Connect) VoteCo, LLC:



Aaron Sobel, Chief Executive Officer and President
AP (Connect) VoteCo, LLC