

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of	)	
	)	
Wuru Telecom, Inc.	)	File No. ITC-214-20200811-00153
	)	
Application for Global or Limited	)	
Global Resale Authority Pursuant to	)	
Section 214 of the Communications	)	
Act of 1934, As Amended	)	

**PETITION TO ADOPT CONDITIONS
TO AUTHORIZATION AND LICENSE**

Pursuant to Executive Order 13913, the National Telecommunications and Information Administration (NTIA) submits this Petition to Adopt Conditions to Authorization and License (Petition) on behalf of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee).¹ Through this Petition, and pursuant to section 1.41 of the Commission’s Rules, the Committee advises the Commission that it has no objection to the Commission approving the above-captioned application, provided that the Commission conditions its approval on the assurance of Wuru Telecom, Inc. (Wuru) to abide by the commitments and undertakings set forth in the February 22, 2021 Letter of Agreement (LOA), a copy of which is attached hereto.²

Section 214 of the Communications Act provides that no carrier may provide telecommunications service to, from, or within the United States until the Commission determines that the present or future public interest, convenience and necessity will be served

¹ Exec. Order No. 13913, § 9(h), 85 Fed. Reg. 19643, 19647-48 (2020). The Executive Order directs the Committee to “assist the [Commission] in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector.” *Id.* § 3(a), 85 Fed. Reg. at 19643.

² 47 C.F.R. § 1.41.

thereby.³ As part of the public interest analysis of section 214 applications, the Commission considers whether any such application raises national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's foreign ownership.⁴ With regard to these concerns, the Commission has long sought the expertise of the relevant Executive Branch agencies and has accorded deference to their expertise when they have identified such concerns in a particular application.⁵

After discussions with representatives of Wuru in connection with the above-captioned application, the Committee has concluded that the additional commitments set forth in the LOA will help ensure that those agencies with responsibility for enforcing the law, protecting the national security, and preserving public safety can proceed appropriately to satisfy those responsibilities.

Accordingly, NTIA on behalf of the Committee advises the Commission that the Committee has no objection to the Commission granting the above-captioned application, provided that the Commission conditions its consent on compliance with the February 22, 2021 LOA attached to this filing.

Respectfully submitted,



Kathy Smith, Chief Counsel

National Telecommunications and
Information Administration
1401 Constitution Avenue, NW
Washington DC 20230
(202) 482-1816

March 10, 2021

³ 47 U.S.C. § 214(a).

⁴ See *Market Entry and Regulation of Foreign-affiliated Entities*, Report and Order, 11 FCC Rcd 3873, 3888, 3955, ¶¶ 38, 216-19 (1995).

⁵ *Id.* at 3955, ¶ 219.



February 22, 2021

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: Wuru Telecom, Inc., ITC-214-20200811-00153 (TT 20-043); Application for authority pursuant to Section 214 of the Communications Act of 1934, as amended, to provide facilities-based and resale-based services between the United States and international points

Dear Sir/Madam:

This Letter of Agreement (“LOA” or “Agreement”) sets forth the commitments that Wuru Telecom, Inc. (“Wuru”) makes 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 Wuru’s applications to the Federal Communications Commission (“FCC”) requesting authority to provide global or limited global facilities-based and resale-based services between the United States and international points pursuant to Section 214 of the Communications Act of 1934, as amended, 47 U.S.C. § 214, and the implementing regulation at 47 C.F.R. § 63.18(e)(1), (2).

Wuru certifies as true and correct, under penalties outlined in 18 U.S.C. § 1001, all statements Wuru 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 this LOA” means the date on which Wuru executes this LOA.

e. “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.

f. “Domestic Communications Infrastructure” (“DCI”) means

- i. Any Wuru system that supports any communications originating or terminating in the United States, 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 of¹, Wuru to provide, process, direct, control, supervise, or manage DC.

g. “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

¹ The phrase “on behalf of,” as used in this paragraph, does not include entities with which Wuru has contracted for peering, interconnection, roaming, long distance, wholesale network access, or other similar arrangements.

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.
- h. “Foreign” means non-United States, or its territories.
- i. “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.
- j. “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.
- k. “Managed Network Service Provider” or “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; 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.
- l. “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.
- m. “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 Wurü.

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

o. “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.

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

q. “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 disclosure of, PII or Sensitive Personal Data;
- 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 Wuru’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 Wuru’s ability to comply with the terms of this LOA.

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

s. “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.

t. “U.S. Records” means Wuru’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 Wuru 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. Wuru 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. Wuru agrees to provide the LEPOC’s PII to USDOJ within 30 days of the Date of this LOA. USDOJ agrees to object or waive objection within 30 days from receiving the LEPOC’s PII.

4. Wuru 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. Under these circumstances, USDOJ and FBI will object or not object to the replacement LEPOC within 30 days of notification.

5. Wuru 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 USDOJ grants an extension.

6. Wuru agrees to implement, either directly or through a vendor, a process to screen newly hired Wuru personnel or any personnel of an approved Outsourced or Offshored service provider performing under an agreement with Wuru. The personnel screening process shall include background investigations, public criminal records checks, or other analogous means to ascertain a person’s trustworthiness. Wuru further agrees to provide USDOJ with a written description of this personnel-screening process within one year after the Date of this LOA, or with its Annual Report, for USDOJ objection or non-objection.

Lawful U.S. Process and Requests for Information

7. Wuru agrees to comply with all applicable lawful interception statutes, regulations, and requirements. Wuru 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 the LOA.

8. Wuru 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. Wuru 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, Wuru 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.

11. Wuru 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 that has not been screened consistent with this LOA, without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

12. Wuru 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. Wuru agrees to refer any requests for U.S. Records, Domestic Communications, or any call content and call data information from a Foreign person that has not been screened consistent with this LOA or a Foreign Government, or 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, Wuru, 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. Wuru agrees not to comply with such requests from Foreign Governments and Foreign persons that have not been screened consistent with this LOA without prior written consent of USDOJ, or an order of a court of competent jurisdiction in the United States.

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

Unauthorized Access and Security Incidents

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

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

18. Wuru agrees to provide, no later than 30 days after receipt of a request by USDOJ, its (1) cybersecurity plans; and (2) Network System Security Plans ("NSSP"). Wuru agrees that its cybersecurity plans will conform with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Wuru further agrees to make modifications to these plans, if reasonably requested by USDOJ, and to work with USDOJ to implement such modifications.

19. Wuru 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 Wuru in the ordinary course of business, and Wuru's plans regarding new contracts or amendments to existing contracts with third-party providers requiring those third parties to notify Wuru 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. Wuru agrees to provide to USDOJ updated network diagrams to include all facilities, devices, Points of Presence (PoPs), and NOCs no later than 30 days after request.

21. Wuru agrees to notify USDOJ at least 30 days prior to changing the location for storage of U.S. Records for USDOJ objection or non-objection. 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 Wuru);
- c. The location where the information is to be stored; and
- d. A description of the physical/logical protections at the new location.

Reporting Incidents and Breaches

22. Wuru agrees to report to USDOJ promptly, and in any event no later than 48 hours, after if 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 U.S. Records, or services provided by Wuru, or referring or relating in any way to Wuru's customers in the United States or its territories;
- c. Unauthorized Access to, or disclosure of, DC in violation of federal, state, or local law; or
- d. Material breach of the commitments made in this LOA.

23. Wuru agrees to require any third-party service provider to disclose to Wuru 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.

24. Wuru 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 72 hours after Wuru has knowledge of, or is informed by a 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. Wuru 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 Wuru, and shall electronically report the matter to the central reporting facility through the following portal: <https://www.cpnireporting.gov>

Principal Equipment

26. Upon request by USDOJ, Wuru agrees to provide a Principal Equipment List for USDOJ objection or non-objection within 90 days of such request. Wuru agrees to consult with USDOJ regarding the format of the Principal Equipment List before submission and agrees to re-submit the Principal Equipment List in a different format if requested by USDOJ. 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. Any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment.
- c. An explanation of Wuru's criteria for including items in the Principal Equipment List, and reasons for excluding any equipment.

27. Wuru agrees to notify USDOJ in writing at least 30 days prior to introducing any new Principal Equipment or modifying any of its Principal Equipment for USDOJ objection or non-objection. USDOJ will object or non-object to such new Principal Equipment or modification to the Principal Equipment within 30 days of receipt of notice.

28. Wuru 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 Wuru within 30 days of receipt of notice.

Change in Ownership and Service Portfolio

29. Wuru agrees to provide USDOJ notice of any changes to its business, including but not limited to corporate structure changes, ownership changes involving five (5) percent or greater equity, 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, but notices of pro forma transactions may be provided concurrently with notice to the FCC. Wuru 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 Wuru's debts.

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

Annual Report

31. Wuru agrees to provide an annual report to USDOJ regarding Wuru'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 Wuru'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;
- c. 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;
- d. A re-identification of the location that Wuru stores U.S. Records;
- e. Recertification of the telecommunications or information services that Wuru provides or confirmation that no additional telecommunications or information services are being offered;
- f. A re-identification of the name of and contact information of the LEPOC;
- g. Whether any of the following were submitted to USDOJ in the previous year: cybersecurity plans/Network System Security Plans; Principal Equipment List; network diagrams.
- h. Certification of compliance with CALEA and any other applicable U.S. lawful interception statutes, regulations, and requirements;

The annual report will be due one year after the Date of the LOA and every year thereafter. Wuru 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 Wuru 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, Wuru agrees to provide USDOJ with paper copies of any annual report, notices, or communications required under this LOA.

Site Visits

32. Wuru agrees to permit USDOJ's requests for site visits and information, and to approve all requests to conduct on-site interviews of Wuru employees.

Miscellaneous

33. Wuru 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.

34. If USDOJ or Wuru believes that changed circumstances warrant modifying or terminating this LOA, USDOJ will engage in discussions with Wuru to determine whether these changed circumstances warrant modification or termination consistent with Executive Order 13913. Rejection of a proposed modification alone shall not constitute evidence of a failure to negotiate in good faith.

35. Wuru agrees that in the event that Wuru breaches the 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 Wuru or its successors-in-interest, in addition to pursuing any other remedy available by law or equity.

36. 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.

37. Wuru 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,



Omar Castillo Cobian
Assistant Secretary