DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
www.dlapiper.com

Nancy Victory
nancy.victory@dlapiper.com
T 202.799.4216
F 202.799.5616

November 12, 2019

VIA IBFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Petition for Declaratory Ruling of Puerto Rico Telephone Company, Inc., ISP-PDR-20170823-00002

Dear Ms. Dortch:

In connection with the above-referenced matter, América Móvil, S.A. de C.V. and Telecomunicaciones de Puerto Rico, Inc., the ultimate and direct parents of Puerto Rico Telephone Company, Inc. ("PRTC"), have agreed with the U.S. Department of Justice ("DOJ") and U.S. Department of Homeland Security to terminate their existing agreement entered into in 2006 as part of WT Docket No. 06-113[1] and to enter into a new agreement with DOJ. The termination agreement and new agreement are enclosed as Attachments 1 and 2. The effective date for the termination agreement and the new agreement ("Effective Date") will be the date the FCC grants the above-captioned petition for declaratory ruling, ISP-PDR-20170823-00002.

PRTC hereby requests that, as of the Effective Date, the Commission remove the condition adopted in WT Docket No. 06-113 requiring compliance with the 2006 agreement. In its place, PRTC requests that the Commission adopt a new condition associated with the new agreement. The requested condition is as follows:

> This authorization and any licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between América Móvil, S.A. de C.V., on behalf of itself and the subsidiaries through which it will hold its interest in Telecomunicaciones de Puerto Rico, Inc., on the one hand, and the U.S. Department of Justice, on the other, dated November 7, 2019, which Agreement is intended to enhance the protection of U.S. national security, law enforcement, and public safety. Nothing in the Agreement is intended to limit any obligation imposed by Federal law or regulation.

[1] *See* Applications of Verizon Communications, Inc. and América Móvil, S.A. de C.V. for Consent to the Transfer of Control of Entities Holding Commission Licenses and Authorizations Pursuant to Section 214 and 310(d) of the Communications Act, *Memorandum Opinion and Order and Declaratory Ruling*, 22 FCC Rcd. 6195 (2007).

Section 6.1 of the new agreement (*see* Attachment 2) directs PRTC to notify the FCC that, provided the FCC adopts the above condition, the DOJ has no objection to the grant of PRTC's above-captioned Petition for Declaratory Ruling.

Please do not hesitate to contact the undersigned counsel for PRTC with any questions regarding this letter.

Respectfully submitted,

DLA Piper LLP (US)

/s/ Nancy Victory

Nancy Victory
Partner

Attachment 1

Termination Agreement for 2006 Agreement

TERMINATION AGREEMENT

This Termination Agreement is made by officials with the authority to bind the U.S. Department of Justice ("DOJ") and the U.S. Department of Homeland Security ("DHS", and together with DOJ, the "U.S. Government Parties"), as well as by official representatives of América Móvil, S.A. de C.V. ("América Móvil") and Telecomunicaciones de Puerto Rico, Inc. ("TELPRI", and together with América Móvil, the "Companies"), in relation to the December 15, 2006, Security Agreement ("2006 Security Agreement") among the U.S. Government Parties and the Companies.

The U.S. Government Parties and the Companies hereby affirm that in connection with a Petition for Declaratory Ruling, FCC File No. ISP-PDR-20170823-00002, América Móvil, TELPRI and DOJ have agreed to enter into an updated Security Agreement, thereby obviating the need to continue the 2006 Agreement. The updated Security Agreement is effective upon the date the FCC grants the above-referenced petition.

Per Section 8.14 of the 2006 Security Agreement, the U.S. Government Parties and Companies herein agree that the 2006 Security Agreement is irrevocably terminated as of the date the updated Security Agreement goes into effect. All of the rights therein are hereby irrevocably relinquished and surrendered; and all obligations and duties owed or required to be performed thereunder are hereby irrevocably waived and released.

This Termination Agreement may be executed in counterparts, and delivery of counterpart signatures may be by facsimile or other electronic means, including ".pdf" transmission.

This Termination Agreement is executed on behalf of the U.S. Government Parties and the Companies:

América Móvil, S.A. de C.V.

Printed Name:
Title:

Nov. 8, 2019
Date

Telecomunicaciones de Puerto Rico, Inc.

Printed Name:
Title:

Nov. 8, 2019
Date

United States Department of Justice

Printed Name: David Plotinsky
Title: Principal Deputy Chief

11/7/19
Date

U.S. Department of Homeland Security

Printed Name: MICHAEL T. DOUGHERTY
Title: A/S FOR BORDER, IMMIGRATION & TRADE POLICY

10.25.19
Date

Attachment 2

New Agreement with DOJ

CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565
EXEMPT FROM DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT

NATIONAL SECURITY AGREEMENT

This AMENDED AND RESTATED NATIONAL SECURITY AGREEMENT ("Agreement") is made on the Agreement Modification Date by and between América Móvil, S.A. de C.V., ("América Móvil"), on behalf of itself and the subsidiaries through which it will hold its interest in Telecomunicaciones de Puerto Rico, Inc. ("TELPRI"), (collectively, "the Companies"), on the one hand, and the U.S. Department of Justice ("DOJ"), referred to herein individually by name or as "a Party" and collectively as "the Parties."

RECITALS

WHEREAS, U.S. communications systems are essential to the ability of the U.S. Government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;

WHEREAS, the U.S. Government has an obligation to the public to ensure that U.S. communications and related information are secure in order to protect the privacy of U.S. persons and to enforce the laws of the United States;

WHEREAS, it is critical to the well-being of the nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States;

WHEREAS, protection of Classified and Sensitive Information is critical to U.S. national security;

WHEREAS, TELPRI has an obligation to protect from unauthorized disclosure the contents of wire and electronic communications;

WHEREAS, TELPRI is the largest telecommunications service provider in Puerto Rico; through its wholly owned subsidiaries Puerto Rico Telephone Company, Inc. ("PRT") and CoquiNet Corporation ("Coqui"), TELPRI provides wireline (domestic and long distance) and wireless telecommunications on the island; and additionally, TELPRI and its Puerto Rico-based companies provide on-island Internet access, private data services and virtual private network ("VPN");

WHEREAS, as disclosed to the Committee on Foreign Investment in the United States ("CFIUS"), TELPRI subsidiary PRT provides telecommunications services to federal government agencies and the Puerto Rico National Guard;

WHEREAS, by Executive Order 13286, the President, pursuant to Section 721 of the Defense Production Act, as amended ("Section 721"), authorized CFIUS to review, for national security purposes, foreign acquisitions of U.S. companies;

WHEREAS, the Companies entered into an earlier agreement to address national security, law enforcement and public safety issues on December 15, 2006;

WHEREAS PRT has filed with the Federal Communications Commission ("FCC") a Petition for Declaratory Ruling pursuant to Section 310 of the Communications Act of 1934, as amended, as reflected in FCC file number ISP-PDR-20170823-00002 seeking to increase the equity ownership and voting control of Carlos Slim Helú and his immediate family in América Móvil and consequently in TELPRI and its subsidiaries; and

WHEREAS after the earlier agreement was signed in 2006, the DOJ has recently concluded that that the evolving nature of the telecommunications industry and improvements in related technology warrant an updated agreement in order to protect the national security.

NOW THEREFORE, the Parties have agreed to modify the prior terms of the earlier agreement to address national security, law enforcement and public safety issues by agreeing to the following modified Agreement Definitions and Terms.

ARTICLE I
DEFINITIONS

As used in this Agreement and the Implementation Plan:

1.1 **"Access" or "Accessible"** means the ability to physically or logically undertake any of the following actions:

(a) read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system, or a network;

(b) read, edit, or otherwise obtain non-public information regarding the Domestic Companies' internal personnel, contractors, service partners, subscribers, or users;

(c) add, edit, or alter information or technology stored on or by software, hardware, a system, or a network; and

(d) 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.).

1.2 **"Agreement Modification Date"** means the date on which the FCC grants the above-referenced Petition for Declaratory Ruling and incorporates the ordering clause set forth in Appendix A of this Agreement .

1.3 **"CALEA"** means the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, *et seq.*

1.4 **"Call Associated Data"** means any information directly related to a Domestic Communication or directly related to the sender or recipient of that Domestic Communication and may include, without limitation, Customer Proprietary Network Information, called party number or other identifier, calling party number or other identifier, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post-cut-through dialed digits, in-band and out-of-band signaling, and party add, drop and hold, and any other "call identifying information," as defined in 47 U.S.C. § 1001(2), as amended or superseded.

1.5 **"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.

1.6 **"Classified Information"** means any information determined pursuant to Executive Order 13526, 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.

1.7 **"Control"** and **"Controls"** means the ability, whether or not exercised, and whether or not exercised or exercisable through the ownership of a majority or a dominant minority of the total outstanding voting securities of an entity, or by proxy voting, contractual arrangements, or other means, to determine, direct, or decide matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding:

(a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;

(b) the dissolution of an entity;

(c) the closing and/or relocation of the production or research and development facilities of the entity;

(d) the termination or nonfulfillment of contracts of the entity;

(e) the amendment of the articles of incorporation or constituent agreement of an entity; or

(f) The Companies' obligations under this Agreement.

1.8 **"Customer Proprietary Network Information" ("CPNI")** has the meaning given it in 47 U.S.C. § 222(h)(1).

1.9 ***"De facto"*** and ***"de jure"*** Control have the meaning provided in 47 C.F.R. § 1.2110.

1.10 **"Domestic Communications" ("DC")** means:

(a) Wire Communications or Electronic Communications (whether stored or not) provided by the Domestic Companies between one U.S. location and another U.S. location; or

(b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) provided by the Domestic Companies that originates from or terminates at a U.S. location.

1.11 **"Domestic Communications Infrastructure" ("DCI")** means:

(a) the network and transmission facilities and equipment (including hardware and software and upgrades as well as platforms) that are owned, operated, or managed by the Domestic Companies to provide, process, direct, control, supervise, or manage Domestic Communications;

(b) the facilities and equipment used by or on behalf of Domestic Companies or any of Domestic Companies to operate, and control their equipment or facilities described in this Section 1.11, and the relevant part of a network of transmission facilities, including satellites owned, operated, or controlled by the Domestic Companies that process Domestic Communications.

1.12 **"Domestic Companies"** means TELPRI and its subsidiaries operating in the United States.

1.13 **"Electronic Communication"** has the meaning given it in 18 U.S.C. § 2510(12).

1.14 **"Electronic Surveillance"** means:

(a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. § 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f);

(b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*;

(c) the acquisition of dialing 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 defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*;

(d) the acquisition of location-related information concerning a telecommunications service subscriber;

(e) the preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and

(f) gaining Access to, or the acquisition or interception of, communications or information as described in (a) through (e) above, and comparable State laws.

1.15 **"Foreign"**, where used in this Agreement, whether capitalized or lower case, means non-U.S.

1.16 **"Governmental Authority"** or **"Governmental Authorities"** means:

(a) any government;

(b) any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau, or political subdivision; and

(c) any court, tribunal, judicial or arbitral body.

1.17 **"Implementation Plan"** means the written blueprint of policies, standards, and procedures that the Domestic Companies will implement in order to comply with this Agreement, subject to DOJ's approval. Certain of the rights and obligations of the Domestic Companies are set forth in further detail in the Implementation Plan, which will be drafted, adopted, and actualized by the Domestic Companies in accordance and consistent with this Agreement pursuant to Section 2.1. The Domestic Companies shall comply with the Implementation Plan, which may be amended from time to time pursuant to Section 2.1 of this Agreement.

1.18 **"Intercept," "Interception,"** or **"Intercepted"** has the meaning defined in 18 U.S.C. § 2510(4).

1.19 **"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. IPDR mainly is used by cable industries and incorporated into CableLabs Data Over Cable Service Interface Specification **("DOCSIS")** protocol.[1] It provides network usage and user information for the network management.

1.20 **"Lawful U.S. Process"** means U.S. federal, state, or local electronic surveillance orders or authorizations, and other orders, legal process, statutory authorizations and certifications for interception of, Access to or disclosure of DC, Call Associated Data, Transactional Data, or Subscriber Information authorized by U.S. law.

1.21 **"Managed Network Service Provider"** means any third party using an end-to-end or managed-services platform to provide any of the following functions for the DCI: operations and management support; corrective and preventative maintenance including intrusive testing; network and service monitoring; network performance, optimization,

[1] DOCSIS is a standard interface for cable modems.

and reporting; network audits, provisioning, and development, and the implementation of changes and upgrades.

1.22 **"Network Operations Center" ("NOC")** means the locations and facilities designated as such by the Domestic Companies for purposes of performing network management, monitoring, maintenance, provisioning or other operational functions for DCI in the United States.

1.23 **"Offshore" or "Offshoring"** means, with respect to DC provided by the Domestic Companies, performing obligations of this Agreement through the use of entities and personnel outside the territorial limits of the United States, whether those entities or personnel are employees of the Domestic Companies or third parties.

1.24 **"Outsource" or "Outsourcing"** means, with respect to DC, supporting the services and operational needs of the Domestic Companies at issue in this Agreement through the use of contractors.

1.25 **"Parties"** has the meaning given it in the Preamble. "Party," singular, means any neutral sole entity that comprises one of the entities within the Parties.

1.26 **"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.

1.27 **"Principal Equipment"** means the hardware and software elements of DCI that are critical for customer authentication, establishment, aggregation, and applicable direction of the flow of Domestic Companies' voice and data connections, whether wireless or wireline, including: network Operations Support Systems (OSS), Network Management Systems, DCI provisioning systems, CALEA equipment, voice call equipment, wireline switches, IP Multimedia System nodes, Mobility Management Entity, critical databases (*e.g.,* customer databases for provisioning and activation of services such as the Policy Charging and Rules Function, Intelligent Networks, Home Location Register, and Home Subscriber Server), packet gateways and critical routers, firewall(s), load balancers, signaling system (SS7 and Diameter) nodes, Software Defined Networking controllers, Radio Access Network (RAN) baseband and smart antenna elements that are responsible for the authentication and cyphering of voice and data sessions, messaging nodes, satellite systems, submarine line terminating equipment, and microwave transport, as applicable, and any non-embedded related software necessary for the proper administration thereof. For the avoidance of doubt, "Principal Equipment" includes the critical hardware and software elements of Domestic Companies' network or any successor technological standard, and does not include any customer premises equipment. These primary electronic components shall include hardware used for a NOC, satellite, earth station, enhanced packet core ("EPC"), broadcast, or cell-site station, and the electronic equipment necessary for the operation of the base station control units ("BSC"), digital TV transmitters, network routers, call servers, circuit switches/softswitches, wired and wireless radio transmitters, and multiplexers, as applicable.

1.28 **"Screened Personnel"** means those persons described in detail in Section 3.12 of this Agreement.

1.29 **"Sensitive Information"** means information that is not Classified Information regarding:

(a) the persons or facilities that are the subjects of Lawful U.S. Process;

(b) the identity of the government agency or agencies serving such Lawful U.S. Process;

(c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance;

(d) the means of carrying out Electronic Surveillance;

(e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process; and

(f) other information that is not Classified Information and is 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."

1.30 **"Subscriber Information"** means information:

(a) of the type referred to and accessible subject to the procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709; or

(b) sought pursuant to the provisions of other Lawful U.S. Process.

1.31 **"The Domestic Companies' U.S. Point of Presence" ("The Domestic Companies' U.S. POP")** means the Domestic Companies' point of presence (POP) in the United States that is subject to the Implementation Plan. The Domestic Companies' U.S. POPs include, but are not be limited to, sites supporting the Domestic Companies' termination, origination, mediation, routing, and/or switching of DC and that are physically located in the United States.

1.32 **"Transactional Data"** means:

(a) any "call identifying information," as defined in 47 U.S.C. § 1001(2), including, without limitation, the telephone number or similar identifying designator associated with a communication;[2]

(b) Internet address or similar identifying designator associated with a communication;

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

(c) the time, date, size, and duration of a communication;

(d) any information relating specifically to the identity and physical/logical address of a subscriber, user, or account payer of the Domestic Companies ;

(e) to the extent associated with a subscriber, user, or account payer of the Domestic Companies, 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

(f) any information indicating, as closely as possible, the physical location to or from which a communication is transmitted.

1.33 **"United States" (or "U.S.")** means the United States of America, including all of its States, districts, territories, possessions, commonwealths, and territorial and special maritime jurisdictions.

1.34 **"United States (or U.S.) Law"** means any U.S. federal, state, or local law or regulation.

1.35 **"Wire Communication"** has the meaning given it in 18 U.S.C. § 2510(1).

1.36 **Other Definitional Provisions**: Other capitalized terms used in this Agreement and the Implementation Plan not defined in this Article shall have the meanings assigned them elsewhere in this Agreement. The definitions in this Agreement are applicable to the singular as well as the plural forms of such terms and to the masculine, feminine, and gender-neutral versions of such terms. Whenever the words "include," "includes," or "including" are used in this Agreement, they shall be deemed to be followed by the words "without limitation." Where a term is specifically defined herein, that definition controls over other definitions, general industry terms of art, or common understandings regarding the meaning for such term.

ARTICLE II
OPERATIONS, FACILITIES, INFORMATION STORAGE, AND ACCESS

2.1 **Implementation Plan**: The Domestic Companies will maintain an Implementation Plan regarding the methods and processes that will be used to ensure compliance with the Agreement. Such Implementation Plan is subject to the DOJ's review and approval every **two (2) years**, with the first review due **ninety (90) days** from the Agreement Modification Date.

(a) The Implementation Plan must require the Domestic Companies to prepare network security policy documents subject to DOJ approval for the matters of interest herein; specifically, information security, 5G, remote access, physical

security, cybersecurity, third-party contractors, Outsourcing and Offshoring, and Syslogs.

(b) The Parties agree to consider in good faith the inclusion of any recommended additions to the Implementation Plan identified by DOJ. Upon agreement of the Parties, the Implementation Plan will include additional requirements and specifications not specified herein, but which support the interests and intent identified in this Agreement (*e.g.*, additional deadline periods). Any such requirements and specifications will become part and parcel of the obligations memorialized in this Agreement once the Implementation Plan is approved and adopted.

2.2 **Operational Requirements**: With respect to the operation of the DCI, the Domestic Companies agree as follows, except where otherwise approved by the DOJ:

(a) **POP**: The Domestic Companies will ensure that any DC with origination and termination points in the United States are routed only within the United States, or otherwise through a third-party point of presence in the United States, in accordance with the Implementation Plan (as defined herein), except for *bona fide* commercial reasons, including, by way of example, (a) as is temporarily necessary to avoid network congestion; (b) as is consistent with least-cost routing practices; or (c) as otherwise exempted by the DOJ. The Annual Report submitted pursuant to Section 4.11 will include a description of the cases in which DC were routed outside of the United States for *bona fide* commercial reasons referenced above, which shall be subject to the third-party audit required under Section 4.12.

(b) **DCI**: All network equipment used for DC shall be located in the United States, except as otherwise permitted under the terms of this Agreement or policies adopted in accordance therewith. All DCI shall be managed, directed, controlled, and supervised by the Domestic Companies.

(c) **NOC**: Except as otherwise approved by DOJ, and with the exception of an existing NOC for the AMX-1 cable, the U.S. NOCs supporting any DCI shall be maintained and remain within the United States. To operate the U.S. NOC(s), the Domestic Companies shall exclusively rely upon Screened Personnel, as defined herein. Should the Domestic Companies wish to rely upon subcontractors to operate the U.S. NOCs, such subcontractors will be subject to pre-approval by the DOJ, except that current subcontractors in use as of the effective date of this Agreement do not require additional approval.

(1) Within **forty-five (45) days** from Agreement Modification Date, the Domestic Companies shall provide the DOJ with a list of the current subcontractors operating the U.S. NOCs.

(2) Should the Domestic Companies wish to establish and/or maintain outside of the United States a NOC supporting any DCI, such NOC would be

subject to non-objection by the DOJ. The Domestic Companies shall submit a notice seeking pre-approval at least **forty-five (45) days** in advance of the establishment of any NOC outside the United States; *provided, however* that if no written objection is provided by the DOJ within such forty-five (45) day objection period, the request to maintain a NOC outside the United States shall be deemed approved. The notice must include a detailed description of the location, facilities, personnel, and operations of the proposed NOC.

(d) **Separation of DC and DCI from the Domestic Companies**: Except to the extent and under conditions concurred by the DOJ in writing or as provided in subsection (c), operational control of DCI, including network administration, maintenance and provisioning, will be restricted to the Domestic Companies' facilities located in the United States, and the Domestic Companies shall generally prohibit remote access from outside the United States to Principal Equipment, any capabilities to conduct electronic surveillance, and operational support systems. The Domestic Companies shall notify the DOJ of any proposed remote access at least **thirty (30) days** in advance, and the DOJ shall have **thirty (30) days** after such notice to review and object to the same. For the avoidance of doubt, if no written objection is provided by the DOJ within the **thirty (30) day** objection period, the request for remote access shall be deemed approved. Should the DOJ object, the remote access at issue will not be actualized. Existing remote access arrangements shall be notified to the DOJ within **thirty (30) days** as of the effective date of this Agreement, and if DOJ has concerns with any existing access arrangement, the Domestic Companies will work in good faith to resolve such concerns.

(e) **CPNI**: The Domestic Companies shall comply with all applicable FCC rules and regulations governing Access to and the storage of CPNI, including notifying the Federal Bureau of Investigation and the U.S. Secret Service as soon as practicable, and in no event later than **seven (7) business days** upon learning that a person or entity without authorization, or in exceeding their or its authorization, has intentionally gained access to, used, or disclosed any of the Domestic Companies' customers' CPNI, or that of a third party used by the Domestic Companies, and shall report the matter to the central reporting facility through the following portal: https://www.cpnireporting.gov/cpni/content/disclaimer.seam

2.3 **Compliance with Lawful U.S. Process**: The Domestic Companies shall take all practicable steps to configure DCI such that it is capable of complying with the CALEA and the Domestic Companies' employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with Lawful U.S. Process, the orders of the President in the exercise of the President's authority under Section 606 of the Communications Act of 1934, as amended (47 U.S.C. § 606), Section 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382), and National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

2.4 **Network and Telecommunications Architecture**: Within **ninety (90) days** from the Agreement Modification Date, the Domestic Companies shall submit to the DOJ an updated comprehensive description of their DCI network and detailed transport network diagrams. These descriptions/diagrams shall include the locations and manufacturers of all Principal Equipment as well as architecture interconnect diagrams, architecture flow diagrams, and architecture context diagrams. The comprehensive description also shall include the following information regarding the POPs, NOCs, colocations and peering points for the DCI:

(a) a description of the plans, processes and/or procedures relating to network management operations that prevent the DCI and DC from being Accessed or controlled from outside the United States;

(b) a description of the placement of NOCs, data centers, and OSS hosting centers,

(c) a description of the Domestic Companies' IP and broadband networks and operation processes, procedures for management control, and their operational processes and procedures for interconnection control and peering relationships with the backbone infrastructures of other service providers; and

(d) a description of any unique or proprietary application, platform, and or capability that supports the operation of the DCI and/or DC.

2.5 **Information Storage and Access**: The Domestic Companies shall make such available in the United States:

(a) stored DC, if such communications are stored by or on behalf of the Domestic Companies for any reason;

(b) any Wire Communication or Electronic Communication (including any other type of wire, voice, or electronic communication not covered by the definitions herein of Wire Communication or Electronic Communication) received by, intended to be received by, or stored in any account of the Domestic Companies' U.S. users, or routed to the Domestic Companies' U.S. POP and stored by or on behalf of the Domestic Companies for any reason;

(c) Transactional Data and Call Associated Data relating to DC if such information is stored by or on behalf of the Domestic Companies for any reason;

(d) billing records relating to the Domestic Companies' customers or subscribers, if such information is stored by or on behalf of the Domestic Companies for any reason, for so long as such records are kept, and at a minimum for as long as such records are required to be kept pursuant to applicable U.S. Law, this Agreement, and the Implementation Plan;

(e) Subscriber Information concerning the Domestic Companies' customers or subscribers, if such information is stored by or on behalf of the Domestic Companies for any reason;

(f) a description of the placement of the Domestic Companies' NOCs, data centers, and OSS hosting centers;

(g) a description of the Domestic Companies' IP/broadband networks and operation processes, procedures for management control, and operational processes and procedures for interconnection control and peering relationships with the backbone infrastructures of other service providers;

(h) a description of any unique or proprietary control mechanisms of the Domestic Companies as well as of the Domestic Companies' operating and administrative software/platforms.

2.6 **Storage Pursuant to 18 U.S.C. § 2703(f)**: Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Governmental Authority within the United States to preserve any of the information enumerated in Section 2.5 of this Agreement, or upon receiving any other preservation request served in compliance with U.S. law, the Domestic Companies shall store such preserved records or other evidence in the United States in the manner and for so long as required by U.S. Law.

2.7 **Mandatory Destruction**: The Domestic Companies shall ensure that the data and communications described in Section 2.5 of this Agreement are stored in a manner not subject to mandatory destruction under any foreign laws. The Domestic Companies shall further ensure that the data and communications described in Section 2.5 of this Agreement shall not be stored by or on behalf of the Domestic Companies outside of the United States.

2.8 **Billing Records**: The Domestic Companies shall store for at least eighteen (18) months post-bill generation all CDRs, CPNI, and other billing records generated that relate to DC and broadband services.

2.9 **Compliance with U.S. Law**: Nothing in this Agreement or the Implementation Plan shall excuse the Domestic Companies from any obligations they may have to comply with U.S. legal requirements for the retention, preservation, or production of information or data.

ARTICLE III
SECURITY AND SECURE FACILITY

3.1 **Location of Secure Facility**: The Domestic Companies shall maintain an appropriately secure facility within the United States within which the Domestic Companies shall:

(a) take appropriate measures to prevent unauthorized Access to data or facilities that contain Classified Information or Sensitive Information, to include the development of appropriate visitation policies regarding visits to the DCI by foreign persons other than employees of the Domestic Companies;

(b) assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or that regularly deal with information identifiable to such U.S. citizens as Sensitive Information:

(1) The citizenship limitation of this Section 3.1(b) of this Agreement shall not apply to those foreign citizens already serving in positions handling or regularly dealing with Sensitive Information as part of their job responsibilities as of the Agreement Modification Date, so long as the names of all such persons are sent to the DOJ for a non-objection decision within **sixty (60) days** of the of the Agreement Modification Date, and so long as the list of such persons is routinely updated and submitted to the DOJ in the Annual Report required by Section 4.11, herein. For the avoidance of doubt, if no written objection is provided by the DOJ within the **sixty (60) day objection period**, the list of such persons shall be deemed approved. Once a foreign citizen is notified to the DOJ, should such person leave his/her position, such person's replacement must comport with the citizenship requirements of Section 3.1(b).

(2) If, after the Agreement Modification Date, the Domestic Companies deem it necessary to assign a foreign citizen to a position referenced in Section 3.1(b) of this Agreement, such party shall seek a waiver from Section 3.1(b)'s U.S. citizenship requirement by sending the PII of the relevant foreign citizen candidate, and an explanation as to why such a waiver is necessary, to the DOJ. Any such waiver request must be submitted to the DOJ at least **thirty (30)** days prior to any assignment of a non-U.S. citizen to any position falling within those outlined in Section 3.1(b). The DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 3.1(b)(2) to object to such request; *provided, however*, that if no objection is made by the DOJ within such thirty (30) day objection period, the waiver request shall be deemed approved. Should the DOJ, within its **thirty (30) day objection period**, seek additional information regarding a waiver request or the foreign citizen candidate at issue, then the DOJ shall make every effort to ensure that such inquiry is reasonable, and the Domestic Companies shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 3.1(b)(2), the DOJ' **thirty (30) day objection period** shall be extended by the number of days it took the Domestic Companies to provide a response. Should the DOJ grant a request to waive the U.S. citizenship requirement of Section 3.1(b) pursuant to Section 3.1(b)(2), the name(s) of the foreign citizen candidate(s) at issue in

that waiver shall be added to the list of persons routinely updated pursuant to Section 3.1(b)(1) and submitted to the DOJ in the Annual Report required by Section 4.11 of this Agreement in a manner clearly identifying such persons as appearing on the list by virtue of a waiver. Once a foreign citizen is the subject of a waiver pursuant to Section 3.1(b)(2), should such person leave his/her position, such person's replacement must comport with the U.S. citizen requirements of Section 3.1(b).

(c) upon the DOJ's request, provide the PII of each person who regularly handles or deals with Sensitive Information;

(d) require that personnel handling Classified Information, if any, shall be eligible for and possess appropriate security clearances prior to handling such information;

(e) provide that the points of contact described in Section 3.5 of this Agreement shall have sufficient authority over any of the Domestic Companies' employees who may handle Classified Information, if any, or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority, and the terms of this Agreement and the Implementation Plan; and

(f) maintain appropriately secure facilities (*e.g.*, offices) for the handling and storage of any Sensitive Information and Classified Information, if any.

3.2 **Measures to Prevent Improper Use or Access**: The Domestic Companies shall take all practicable measures to prevent the use of or Access to the equipment or facilities supporting those portions of the DCI necessary for conducting Electronic Surveillance where such use or Access would violate any U.S. Law, the terms of this Agreement or the Implementation Plan. These measures shall include technical, organizational, personnel-related policies and written procedures, as well as necessary implementation plans and physical security measures.

3.3 **Access by Foreign Government Authorities**: Without the prior express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States, the Domestic Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to, DC, Call Associated Data, Transactional Data, or Subscriber Information, if such information is stored in the United States, to any person if the purpose of such disclosure or Access is to respond to the legal process or the request of or on behalf of a Foreign Government Authority, identified representative, or a component or subdivision thereof. Any such requests or submissions of legal process described in this Section 3.3 shall be reported to the DOJ as soon as possible and in no event later than **five (5) business days** after such request or legal process is received by and known to management of the Domestic Companies, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. The Domestic Companies shall take reasonable measures to ensure that mechanisms are in place for management to promptly report all such requests or submission of legal process described in this Section 3.3. The Security Officer, as

defined in Section 3.8, shall review management positions and operating procedures of Domestic Companies to ensure the company is appropriately situated so that the legal process described in this Section 3.3 is properly disclosed to the appropriate management personnel.

3.4 **Disclosure to Foreign Government Authorities**: The Domestic Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

(a) Classified Information or Sensitive Information; or

(b) Subscriber Information, Transactional Data, Call Associated Data, or a copy of any Wire Communication or Electronic Communication, intercepted or acquired pursuant to Lawful U.S. Process

to any Foreign Government Authority, identified representative, or a component or subdivision thereof without satisfying all applicable U.S. federal, state, and local legal requirements pertinent thereto, and without obtaining the prior express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. The Domestic Companies shall notify the DOJ of any requests or any legal process submitted to the Domestic Companies by a Foreign Government Authority, identified representative, or a component or subdivision thereof for communications, data, or information identified in this Section 3.4. The Domestic Companies shall provide such notice to the DOJ as soon as possible, and in no event later than **five (5) business days** after such request or legal process is received and known by management of the Domestic Companies, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. The Domestic Companies shall take reasonable measures to ensure that mechanisms are in place for management to promptly learn of all such requests or submission of legal process described in this Section 3.4.

3.5 **Law Enforcement Points of Contact ("LE POCs")**: Within **thirty (30) days** after the Agreement Modification Date, the Domestic Companies shall designate LE POCs within the United States with the authority and responsibility for accepting and overseeing the Domestic Companies' compliance with Lawful U.S. Process. **Within that same period of time**, the Domestic Companies shall notify the DOJ of the designation of the LE POCs, and include in such notice the PII for the LE POCs.

(a) Thereafter, the Domestic Companies shall notify the DOJ of any change in the designation(s) for LE POCs within **ten (10) business days** of such change. Any notice of a new LE POC shall include the PII for the newly designated individual.

(b) The LE POCs shall be resident U.S. citizens who are eligible for appropriate U.S. security clearances, except as otherwise approved in advance by DOJ. The Domestic Companies shall cooperate with any request by a government entity within the United States regarding a designated LE POC's availability for a background check and/or a security clearance process.

(c) The LE POCs will be required to be available twenty-four (24) hours per day, seven (7) days per week, and shall be responsible for accepting service and maintaining the security of:

(1) Sensitive and Classified Information, if any, and subject to subsection (d); and

(2) any CALEA request or Lawful U.S. Process for Electronic Surveillance served upon the Domestic Companies, and the information pertaining thereto, including the content of the results from executing the Lawful U.S. Process, in accordance with the requirements of U.S. Law.

3.6 **Security of Lawful U.S. Process, Sensitive Information, and Classified Information**: The Domestic Companies shall protect the confidentiality and security of all CALEA requests and Lawful U.S. Process served upon them, and the confidentiality and security of Classified Information, if any, and Sensitive Information in accordance with U.S. Law. If the individuals identified in Section 3.5 and Section 3.8 of this Agreement are not eligible for appropriate U.S. security clearances and those individuals are approved in advance by DOJ, the Domestic Companies shall include in the Information Security Plan under Section 3.10 a plan detailing how the Domestic Companies will receive and handle Classified Information in accordance with applicable U.S. legal authority, and the terms of this Agreement.

3.7 **Access to Classified or Sensitive Information**: Nothing contained in this Agreement or the Implementation Plan shall limit or affect the authority of a Government Authority within the United States, under that agency's jurisdiction, to grant, deny, modify, or revoke the Domestic Companies' Access to Classified and Sensitive Information.

3.8 **Designation of Security Officer and/or Technical Compliance Officer ("SOTCO" or "Security Officer")**: The Domestic Companies must designate and maintain a SOTCO. The SOTCO will have the appropriate authority and skills to implement the terms of this Agreement and to address security concerns identified by the DOJ. The SOTCO shall have the appropriate senior-level corporate authority within the Domestic Companies to perform his/her duties under this Agreement and the Implementation Plan. The SOTCO shall possess the necessary resources and skills to enforce this Agreement and to act as a liaison to the DOJ regarding compliance with this Agreement and the Implementation Plan and to address any national security issues arising during the Domestic Companies' due course of business. The Domestic Companies shall provide the SOTCO with Access to the Domestic Companies' business information that is necessary for the SOTCO to perform his/her duties.

(a) The Domestic Companies shall designate the initial SOTCO to the DOJ within **forty-five (45) days** of the Agreement Modification Date, and thereafter shall provide at least **fourteen (14) days'** notice of a SOTCO's departure, and **thirty (30) days' prior notice** of a new SOTCO designation. The Domestic Companies

shall not maintain a vacancy or suspension of the SOTCO position for a period of more than **sixty (60) days**.

(b) All SOTCO designations shall be subject to the DOJ's review and non-objection, and the Domestic Companies shall reasonably address any concerns raised by the DOJ regarding the selection and identity of the SOTCO. For the avoidance of doubt, if no written objection is provided by the DOJ within **thirty (30) days**, the SOTCO designation shall be deemed approved.

(c) With respect to the SOTCO's qualifications, and except as otherwise approved in advance by DOJ, he/she must:

(1) be a resident U.S. citizen who possesses U.S. citizenship;

(2) if not already in possession of a U.S. security clearance, shall be eligible, at the sole discretion of the DOJ, to hold such security clearances immediately upon appointment;

(3) be subject to the screening process described in Section 3.13 of this Agreement;

(4) reside in the United States, in a location that permits and supports the SOTCO's efficient and successful fulfillment of his/her duties and obligations under this Agreement and the Implementation Plan; and

(5) be a corporate officer with appropriate authority, skills, and resources to enforce this Agreement.

3.9 **SOTCO Responsibilities and Duties**: The responsibilities and duties of the SOTCO shall include, at least, each of the following:

(a) Providing the DOJ the Annual Report required of the Domestic Companies under Section 4.11 of this Agreement;

(b) Developing and maintaining the Implementation Plan, along with and the Domestic Companies' Information Security Plan (Section 3.10), Access-or-disclosure requirements (described in Sections 3.2, 3.3, and 3.4); Outsourcing and Offshoring Control and Access Policy (Section 3.11); personnel screening process requirements (described in Sections 3.12 and 3.13), and other policies generally discussed herein (*e.g.*, regarding visitation of the secure facility (Section 3.1(a)) to promote full compliance with this Agreement;

(c) Implementing all aspects of compliance with this Agreement and all corporate policies, procedures, and plans to promote and ensure compliance with this Agreement;

(d) Providing interim reports to the DOJ mandated by this Agreement;

(e) Being aware of, and reporting to the DOJ, changes to corporate structure or operations that would reasonably be deemed to have an effect on the terms or operation of this Agreement;

(f) Being available upon reasonable notice for discussions with the DOJ relating to the enforcement of and compliance with this Agreement or any other issue involving national security;

(g) Ensuring procedures are in place for the Domestic Companies to comply with Lawful U.S. Process in an expeditious, effective, and unimpeded fashion; and

(h) Acting as the liaison and point of contact for the Domestic Companies with the DOJ.

3.10 **Information Security Plan**: Following the Agreement Modification Date, the Domestic Companies shall create, amend, maintain, or adapt an information security plan that, as further expanded upon and explained in the Implementation Plan, at the very least:

(a) Takes appropriate measures to prevent unauthorized Access to DC and DCI and/or facilities that might contain Classified or Sensitive Information;

(b) Ensures assignment of U.S. citizens to positions for which screening is contemplated, except as provided for in Section 3.12(e);

(c) Assigns personnel who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information to positions that handle or that regularly deal with information identifiable to such persons as Sensitive Information;

(d) Upon request from the DOJ, provides to DOJ the PII and other relevant requested identifier information of each person who regularly handles or deals with Sensitive Information;

(e) Requires that personnel handling Classified Information shall have been granted appropriate security clearances consistent with Executive Orders 12968 and 13467 and other applicable law;

(f) Ensures that the LE POCs described in Section 3.5 of this Agreement shall have sufficient authority over any employees or contractors of the Domestic Companies who may handle Classified Information or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;

(g) Ensures that the disclosure of or Access to Classified Information or Sensitive Information is limited to those who have appropriate security clearances and authority;

(h) Identifies the types of positions that require screening pursuant to this Agreement, the required rigor of such screening by type of position, and the criteria by which

the Domestic Companies will accept or reject Screened Personnel (as defined in Section 3.12);

(i) Maintains appropriately secure facilities (*e.g.*, offices, communications centers, network operations centers, etc.) within the United States for the handling and storage of any Classified Information or Sensitive Information; and

(j) Describes the plan referenced in Section 3.6.

3.11 **Outsourcing and Offshoring Control and Access Policy**:

(a) The Domestic Companies shall not Outsource or Offshore functions covered by this Agreement to an entity that is not within the definition of "the Domestic Companies" under this Agreement, except pursuant to the Outsourcing and Offshoring Control and Access Policy adopted pursuant to this Agreement and the Implementation Plan, outlined in Section 2.1.

(1) Where the Domestic Companies already are Outsourcing or Offshoring functions covered by this Agreement, such Outsourcing or Offshoring functions shall be considered exempt from this subsection's prohibition.

(2) In order to assess future compliance with Section 3.11(a), the Domestic Companies shall submit to the DOJ a notice of current Outsourcing and Offshoring providers within **sixty (60) days** of the Agreement Modification Date.

(b) No later than **ninety (90) days** after the Agreement Modification Date, the Domestic Companies will adopt and implement an Outsourcing and Offshoring Control and Access Policy. The Domestic Companies shall consult with the DOJ regarding the memorialization, design, and implementation of such policy, and shall reasonably address any concerns raised by the DOJ with respect to such memorialization, design, and implementation. Further, such policy shall require the Domestic Companies to provide the DOJ **forty-five (45) days' prior notice** of any proposed new Outsourcing or Offshoring, and the right of the DOJ to object within **thirty (30) days** of receipt of such notice to the proposed Outsourcing or Offshoring. For the avoidance of doubt, if no written objection is provided by the DOJ within the **thirty (30) day** objection period, the proposed Outsourcing or Offshoring shall be deemed approved.

(1) Except for exempted Outsourcing arrangements under Section 3.11(a)(1), the Domestic Companies shall not Outsource or Offshore functions involving DC, Access to Classified Information, Sensitive Information, or Lawful U.S. Process; and the Domestic Companies' Outsourcing and Offshoring Control and Access Policy may not provide for such Outsourcing/Offshoring.

(2) All new Outsourcing and Offshoring arrangements shall be subject to DOJ prior notice and opportunity to object under the Domestic Companies' Outsourcing and Offshoring Control and Access Policy, which shall include logical and physical controls (such as restricted access methods and background screening).

(3) The Outsourcing and Offshoring Control and Access Policy may address classes of Outsourcing or Offshoring contracts of a routine and non-sensitive nature to be excluded from Section 3.11(b)'s notice-and-opportunity to object requirement.

3.12 **Screening of Personnel**: The Domestic Companies shall maintain and implement a screening process to ensure compliance with all personnel screening process requirements agreed to herein and in the Implementation Plan. The Domestic Companies will require screening for persons in at least the following circumstances:

(a) All employees who have Access to Classified Information

(b) All employees who have Access to Sensitive Information;

(c) All employees who have Access to DCI to monitor the content of DC;

(d) All employees who have the ability to monitor personnel with limited access to DC under this subsection;

(e) Nothing in this Section 3.12 shall be read to apply the screening requirements to the Domestic Companies' existing employees described in subsections (a) through (d) above or to customers (or their agents) obtaining their own data.

Upon satisfactory completion of the screening process requirements set forth in this Agreement, or pursuant to Section 3.12(e) above), such persons shall be considered "**Screened Personnel.**" For the avoidance of doubt, the screening requirements required by this Section 3.12 shall be generally consistent with those previously approved by DOJ and implemented by the Domestic Companies. The Domestic Companies will cooperate with any reasonable notice by the DOJ to provide additional information necessary for an enhanced background investigation to be conducted by the DOJ with respect to identified Screened Personnel.

3.13 **Screening Process Requirements**: The screening process undertaken pursuant to Section 3.12 and this Section 3.13 of this Agreement shall be implemented through a reputable third party, and shall specifically include a background check in addition to a criminal records' check. The Domestic Companies shall consult with the DOJ on the screening procedures utilized by the reputable third party and shall provide to the DOJ a list of the positions subject to screening no later than **ninety (90) days** after the Agreement Modification Date. Thereafter, the Domestic Companies shall notify the DOJ of changes to the list of positions subjected to screening (*i.e.*, either adding to or removing classes of positions) within **sixty (60) days** of such change.

(a) The Domestic Companies shall utilize the criteria identified pursuant to Section 3.12 of this Agreement to screen personnel, shall report the results of such screening on a regular basis to the Security Officer, and shall, upon request, provide to the DOJ all the information collected through the screening process of each candidate. Candidates for these positions shall be informed that the information collected during the screening process may be provided to the DOJ, and the candidates shall consent to the sharing of this information with the DOJ. In addition:

(1) Subject to the exception in Section 3.12(e), the Domestic Companies shall assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.12(a).

(2) The Domestic Companies may Outsource or Offshore positions for which screening is contemplated pursuant to Section 3.12(d). With respect to Outsourced or Offshored personnel, the Domestic Companies shall ensure that such personnel are subject to restricted Access methods and background screening requirements under the terms of the Outsourcing and Offshoring Control and Access Policy, in accordance with Section 3.11 of this Agreement.

(3) The Domestic Companies shall consult with the DOJ regarding the screening procedures to be used and the positions subject to screening. The Domestic Companies shall reasonably address any concerns the DOJ may raise with respect to such screening procedures. The Domestic Companies shall use the criteria identified in Section 3.12 and this Section 3.13 of this Agreement to identify the personnel to be screened.

(4) The Domestic Companies shall cooperate with requests by the DOJ, or any U.S. Government Authority, desiring to conduct any further background checks. Individuals who are rejected pursuant to such further background checks by the DOJ or a U.S. Government Authority shall not be permitted to perform functions that would require screening under this Agreement.

(5) The Domestic Companies shall rescreen Screened Personnel **every seven (7) years**. The Domestic Companies shall maintain records relating to the status of Screened Personnel, and shall provide such records, upon request, to the DOJ.

(b) Any records or other information relating to individual persons provided to or obtained by the DOJ in connection with this Agreement, including implementation and results of Screening Requirements outlined in Section 3.12 and this Section 3.13 of this Agreement, shall be maintained in a secure and confidential manner strictly in accordance with applicable law.

ARTICLE IV
AUDITING, REPORTING AND NOTICE

4.1 **Notice of Obligations**: The Domestic Companies shall instruct appropriate officers, employees, contractors and agents as to their obligations under this Agreement and the Implementation Plan, and issue periodic reminders of such obligations to such persons. Records of such instructions shall be maintained by the Security Officer.

4.2 **Reporting of Incidents**: The Domestic Companies shall request that employees, contractors, and agents alert management of the Domestic Companies of any information that reasonably indicates the following occurred:

(a) a breach of this Agreement or the Implementation Plan;

(b) unauthorized or improper Access to or disclosure of DC, or the unauthorized or improper conduct of Electronic Surveillance carried out in violation of U.S. Law;

(c) Access to or disclosure of CPNI or Subscriber Information in violation of U.S. Law (except for violations of FCC regulations relating to improper use of CPNI); or

(d) improper Access to or disclosure of Classified Information or Sensitive Information.

The Domestic Companies shall take all practicable steps under the Implementation Plan to ensure that they notify the DOJ if the Domestic Companies' management acquires information about such incidents. The Domestic Companies' notification shall be made promptly and in any event no later than **ten (10) calendar days** after the Domestic Companies' management acquires such information. Further, the Domestic Companies shall lawfully cooperate in investigating the matters pertaining to such notice. The Domestic Companies need not report information where its disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

4.3 **Notice of Decision to Store Information Outside the United States**: The Domestic Companies shall provide the DOJ with **at least thirty (30) days' prior written notice** regarding the storage outside of the United States by the Domestic Companies or any entity with which the Domestic Companies have contracted or made other arrangements for data or communications processing or storage of DC, Transactional Data, Call Associated Data, Subscriber Information, CDRs, CPNI, or other billing records. Upon receipt of such a notice, the DOJ shall have **thirty (30) days** to object to the Domestic Companies' notified plans. For the avoidance of doubt, if no written objection is provided by the DOJ within the **thirty (30) day** objection period, the proposed storage of information outside the United States shall be deemed approved. Such notice shall, at a minimum:

(a) include a description of the type of information to be stored outside the United States;

(b) identify the custodian of the information (even if such custodian is one of the Domestic Companies);

(c) identify the location where the information is to be stored; and

(d) identify the factors considered in deciding to store the information outside of the United States.

4.4 **Notice of Decision to Use Foreign-Located DCI**: The Domestic Companies shall provide DOJ **forty-five (45) days' advance written notice** if the Domestic Companies plan to locate DCI outside of the United States. Upon receipt of such a notice, the DOJ shall have **forty-five (45) days** to object to the Domestic Companies' notified plans. For the avoidance of doubt, if no written objection is provided by the DOJ within the **forty-five (45) day** objection period, the proposed use of foreign-located DCI shall be deemed approved. Such notice shall at a minimum:

(a) include a description of the facilities to be located outside the United States and a description of the functions of the facilities;

(b) identify the location where the facilities are to be;

(c) identify the factors considered in making the decision; and

(d) identify the security provisions taken by the Domestic Companies to protect DC and DCI.

4.5 **Outsourcing Third Parties**: If the Domestic Companies Outsource to third parties any function covered by this Agreement or the Implementation Plan, the Domestic Companies shall take reasonable steps to ensure that those third parties comply with the applicable terms of this Agreement and Implementation Plan for purposes of providing such Outsourced function(s); and the Domestic Companies' Outsourcing and Offshoring Control and Access Policy (Section 3.11) shall memorialize this requirement. The reasonable steps that must be taken shall include:

(a) The Domestic Companies including in the contracts of such third parties, executed on or after the Agreement Modification Date (including, for the avoidance of doubt, the subsequent renewal or extension of any contracts with Outsourcing third parties with which the Domestic Companies have a contract as of the Agreement Modification Date), written provisions requiring that such third parties comply with all applicable terms of the Agreement and Implementation Plan;

(b) The Domestic Companies taking other reasonable, good-faith measures to ensure that such third parties are aware of, agree to comply with, and are bound by the applicable obligations under this Agreement and Implementation Plan (*e.g.*, providing copies of and training regarding the Agreement and Implementation

Plan to such third parties, and requiring acknowledgement forms with respect to their obligations from such third parties, *etc.*);

(c) If the Domestic Companies' management learns that an Outsourcing third party or the Outsourcing third party's employee has violated an applicable provision of this Agreement or the Implementation Plan, the Domestic Companies shall notify the DOJ as promptly as practicable, and in no event later than **seven (7) days** of learning of such violation.

(i) Upon such notification, and in consultation with the DOJ, the Domestic Companies will take the steps necessary to rectify the situation, which steps may include, among others, terminating the arrangement with the Outsourcing third party, initiating and pursuing litigation or other remedies at law and equity, and/or assisting and cooperating with the DOJ in pursuing legal and equitable remedies.

4.6 **Access to Information**: In response to reasonable requests made by the DOJ, the Domestic Companies shall provide Access to information concerning technical, physical, management, or other security measures and other reasonably available information requested by the DOJ to assess compliance with the terms of this Agreement and the Implementation Plan.

4.7 **DOJ Visits and Inspections**: Upon reasonable notice and during reasonable business hours, the DOJ may visit and inspect any part of the Domestic Companies' DCI, secure facilities, corporate offices in the United States, and such other facilities that the parties and the DOJ may agree upon in writing are relevant to this Agreement for the purpose of verifying compliance with the terms of this Agreement and the Implementation Plan. The Domestic Companies may have appropriate employees accompany the DOJ representatives throughout any such inspection.

4.8 **DOJ Access to Personnel**: Upon reasonable notice from the DOJ, the Domestic Companies will make available for interview officers or employees of the Domestic Companies in order to verify compliance with this Agreement and the Implementation Plan. The Domestic Companies also agree to work in good faith to make available to the DOJ contractors for this same purpose.

4.9 **Change in Service Portfolio**: The Domestic Companies agree that upon request they will inform the DOJ of any material changes to their current services portfolio since the last Annual Report.

4.10 **Managed Network Service and Principal Equipment Providers**: No later than **sixty (60) days** after the Agreement Modification Date, the Domestic Companies shall provide the DOJ with a list of names of all Managed Network Service Providers and Principal Equipment providers, including entities that perform any maintenance, repair, or replacement that could result in any material modification to the Principal Equipment or systems or software used with or supporting the Principal Equipment. Such list shall not only identify the Managed Network Service Provider or Principal Equipment, but also

identify the manner/type of service offered. The Domestic Companies shall notify the DOJ at least **thirty (30) days** before using any new Managed Network Service Provider or Principal Equipment provider not previously identified to the DOJ or where there will be changes in the service offerings/support from already identified Managed Network Service Providers and Principal Equipment Providers (*i.e.*, an already identified provider will now be offering support in a previously unidentified way). The DOJ shall approve or disapprove any such request within **thirty (30) days** of receipt, unless otherwise delayed by awaiting responses to inquiries for further information from the Domestic Companies, in which event the DOJ shall be afforded additional time to approve or disapprove any request sent to the DOJ under this Section 4.10. The DOJ's additional time to approve or disapprove shall be either the original thirty (30)-day window extended by the number of days the Domestic Companies took to provide a response or **seven (7) days** after a response from the Domestic Companies is received, whichever is greater. For the avoidance of doubt, if no written objection is provided by the DOJ within the thirty (30) day objection period, the proposed Managed Network Service Provider or PE vendor shall be deemed approved.

(a) In the event of an emergency, as determined by the SOTCO, such as an instance requiring immediate maintenance or repair of facilities and use of a service or equipment for which the necessary Managed Network Service Provider or Principal Equipment supplier has not already been notified to the DOJ, the Domestic Companies may utilize the provider or supplier, provided that the Domestic Companies provide notice to the DOJ as promptly as practicable, and in no event longer than **three (3) business days** after the initial use of the supplier or provider. The Domestic Companies may continue to utilize the provider or supplier, provided that the DOJ does not object within **thirty (30) days** of notification, or within the additional time necessary for the Domestic Companies to answer the DOJ's questions, as outlined for the usual process in Section 4.10.

(b) The Annual Report submitted pursuant to Section 4.11 will include a description of the emergencies determined under Section 4.10(a), which shall be subject to the third-party audit required under Section 4.12.

4.11 **Annual Report**: On or before the yearly anniversary of the Agreement Modification Date, a designated senior corporate officer of the Domestic Companies shall submit to the DOJ a report assessing the Domestic Companies' compliance with the terms of this Agreement and the Implementation Plan for the preceding twelve (12)-month period. The report shall at a minimum include:

(a) a copy of the policies and procedures adopted to comply with this Agreement and the Implementation Plan;

(b) a summary of the changes, if any, to such policies and procedures, and the reasons for those changes;

(c) a summary of any known acts of non-compliance with the terms of this Agreement and the Implementation Plan, 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;

(d) an identification of any other issues that could affect the effectiveness of or compliance with this Agreement or the Implementation Plan;

(e) a list of all of the notices submitted to the DOJ during the prior year;

(f) a current list of all Managed Network Service Providers and Principal Equipment providers, including the manner/type of support from each;

(g) updated network security policies and implementation procedures;

(h) a detailed list of the Domestic Companies' services, including any modifications from the previous year and the date upon which the modification became effective;

(i) identification of any material information with respect to this Agreement not specifically identified in this Section 4.11;

(j) identification of material cybersecurity incidents, in accordance with the Implementation Plan, to include material malicious and persistent network attacks, enterprise intrusions/unauthorized Access, viruses, phishing electronic-mail ("e-mail") messages, and/or similar threats;

(k) an identification of the security incidents noted pursuant to Section 4.2 of this Agreement and;

(l) a list of all foreign citizen personnel who, as of the date of the Annual Report, either remain working in the positions and/or capacities already notified to the DOJ pursuant to Sections 3.1(b)(1) of this Agreement or who need to be added to the list pursuant to Sections 3.1(b)(2) of this NSA.

4.12 **Annual Third-Party Audit**: The Domestic Companies shall retain and pay for a neutral third party technical engineer or subject matter expert to objectively audit the Domestic Companies' compliance with this Agreement every **two (2) years**, provided that the DOJ may request that the Domestic Companies commission an audit during the interim year between standard audit reports should the need arise, as determined by the DOJ. Should the DOJ request an interim audit, every attempt will be made to tailor the scope of that audit to those areas of most interest to the DOJ.

(a) The final audit report for the first audit commissioned under this section shall be due **one (1) year** from the date of DOJ's notice to the Domestic Companies approving the Implementation Plan, with the final reports for each subsequent audit due every **two (2) years** thereafter (*e.g.*, the second final audit report would be due **three (3) years** after the Implementation Plan's approval date; the third, five years after; *etc.*). Should the DOJ request an interim audit, that request shall have no bearing on the due date for the audit otherwise due under this Section

4.12 at the end of the relevant two (2)-year period between standard audits, unless otherwise waived by the DOJ.

(b) The Domestic Companies shall provide notice of, and terms of reference for, their selected auditor to the DOJ, which shall have an opportunity to review and object to the selected auditor within **thirty (30) days** of receiving such notice. In the event of a DOJ objection to a selected auditor, the Domestic Companies shall work in good faith to resolve such objection. For the avoidance of doubt, if no written objection is provided by the DOJ within the **thirty (30) day** objection period, the proposed auditor shall be deemed approved.

(c) The Domestic Companies shall provide to the DOJ a copy of the contract with the selected auditor, which shall include terms defining the scope and purpose of the audit. The DOJ shall have the right to review and comment on such terms. In the event of receiving comments from the DOJ on an audit's terms, the Domestic Companies shall work in good faith to resolve the comments and requests for changes and/or insertions by the DOJ.

(d) Through their contract with the selected auditor, the Domestic Companies shall ensure that all reports generated by the auditor are provided promptly to the DOJ.

(e) At a minimum, the terms defining the scope and purpose of the audit shall include:

(1) Authority for the auditor to review and analyze the Domestic Companies' overall compliance with this Agreement, and the authority to review and evaluate the adequacy and implementation of the policies and procedures necessary to comply with this Agreement, including but not limited to:

(i) Implementation Plan;

(ii) CALEA;

(iii) Access control policies;

(iv) Information Security Plan;

(v) Outsourcing and Offshoring Control and Access Policy;

(vi) Screening process; and

(vii) Process for seeking approval for new Managed Network Service Providers and Principal Equipment Vendors.

(2) Authority for the auditor to conduct a reasonable number of unannounced inspections of the Domestic Companies' facilities.

4.13 **Network Changes**: The Domestic Companies will report to the DOJ any major network provisions or upgrades and changes to Principal Equipment suppliers, Managed Network Service Providers, and third-party contractors within **thirty (30) days** of completing the change.

4.14 **Control of the Domestic Companies**: The Domestic Companies shall promptly provide to the DOJ written notice and copies of any filing(s) with the FCC or any other governmental agency relating to the *de jure* or *de facto* Control of the Domestic Companies, except for filings with the FCC for assignments or transfers of Control that are *pro forma*.

4.15 **Notices**: All communications or other notices relating to this Agreement or the Implementation Plan shall be made by electronic mail and may also be made in any manner and form discussed herein, to the individuals identified herein or to such persons notified to the Parties in the future as updated points of contact with respect to this Agreement. All communications or other notices relating to this Agreement or the Implementation Plan shall be deemed given as of the date and time at which the communication is received by the DOJ's email account and:

(a) when delivered personally;

(b) if by facsimile, upon transmission with confirmation of receipt by the receiving party's facsimile terminal;

(c) if sent by documented overnight courier service, on the date delivered; or

(d) if sent by mail, **five (5) business days** after being mailed by registered or certified U.S. mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the Parties may designate in accordance with this Section 4.15:

For the DOJ:

Eric Johnson
Deputy Chief, Compliance
Foreign Investment Review Section
National Security Division, U.S. Department of Justice
Three Constitution Square
175 N Street NE
Washington, DC 20530
Eric.Johnson@usdoj.gov

For the Foreign Investment Review Section:
cfius@usdoj.gov
FIRS-TT@usdoj.gov

Courtesy electronic copies of all notices and communications will also be sent to the following or individuals identified in the future to the Domestic Companies by DOJ: Hunter Deeley (hunter.deeley@usdoj.gov).

For América Móvil:

Alejandro Cantu
General Counsel
América Móvil, S.A.B. de C.V.
Lago Zurich 245, Edificio TELCEL
Piso 16 Col. Ampliación Granada,
Ciudad de México 11529
acantu@americamovil.com

For TELPRI and PRT:

Francisco J. Silva
General Counsel
Puerto Rico Telephone Company, Inc.
1515 F.D. Roosevelt Avenue
Guaynabo, PR 00968
fsilva@claropr.com

With a copy to:

Nancy J. Victory
DLA Piper LLP
500 Eighth Street, NW
Washington, DC 20004
Nancy.victory@dlapiper.com

ARTICLE V
FREEDOM OF INFORMATION ACT EXEMPTION

5.1. **Protection of Information**: Information provided by the Companies pursuant to this Agreement, or otherwise obtained by the DOJ in accordance with this Agreement, is intended to be accorded confidential treatment consistent with Section 721 and 31 C.F.R. § 800.702.

ARTICLE VI
NON-OBJECTION BY THE DOJ

6.1 **FCC Approval**: Within **two (2) business days** of the execution of this Agreement by all Parties, PRT shall promptly notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Appendix A to this Agreement, the DOJ has no

comment to the grant of PRT's Petition for Declaratory Ruling, pursuant to Section 310 of the Communications Act of 1934, as amended, filed with the FCC identified as file number ISP-PDR-20170823-00002. The DOJ shall thereafter promptly file a letter with the FCC confirming that it has no comment or objection.

6.2 **Future Applications**: Nothing in this Agreement or the Implementation Plan shall preclude the DOJ from opposing, formally or informally, any FCC application by the Domestic Companies to transfer their FCC license(s) to a third party or for any other authority. The DOJ reserves the right to seek additional or different terms that would, consistent with the public interest, address any threat to their ability to enforce the laws, preserve the national security and protect the public safety raised by the transactions underlying such applications or petitions.

ARTICLE VII
MISCELLANEOUS PROVISIONS

7.1. **Obligations of América Móvil**: América Móvil shall direct the Domestic Companies to comply with this Agreement.

7.2. **Right to Make and Perform Agreement**: The Companies represent that they have and shall continue to have throughout the term of this Agreement the authority and full right to enter into this Agreement and perform the obligations hereunder, and that this Agreement is a legal, valid, and binding obligation of the Companies and is enforceable in accordance with its terms.

7.3 **United States Government Remedies:** Each of the Companies acknowledges that, if it fails to comply with any of the terms of this Agreement, the DOJ or any other appropriate United States Government authority may seek any and all remedies available under applicable law, including injunctive or other judicial relief, and remedies under Section 721 and 31 C.F.R. Part 800. The taking of any action by the DOJ in the exercise of any remedy shall not be considered as a waiver by the DOJ of any other rights or remedies. Nothing in this Agreement is intended to create rights to damages enforceable at law by the Companies against the DOJ, nor to limit any rights the DOJ may have under law or regulation.

7.4 **Headings**: The Article headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement.

7.5 **Other Laws**: Nothing in this Agreement is intended to limit or alter or constitute a waiver of:

(a) any obligation imposed on the Companies, their Personnel, or their agents by any U.S. Law;

(b) any enforcement authority available under any U.S. Law;

(c) the sovereign immunity of the United States;

(d) any authority or jurisdiction the U.S. Government may possess over the activities of the Companies, their Personnel, or their agents located within or outside the United States; or

(e) any rights of the Companies, their Personnel, or their agents under the U.S. Constitution, any state constitution, or any U.S. Law. Nothing in this Agreement is intended to or is to be interpreted to require the Companies, their Personnel, or the DOJ to violate any applicable U.S. Law. Likewise, nothing in this Agreement limits the right of the U.S. Government to pursue criminal or civil sanctions or charges against the Companies or their Personnel in an appropriate case, and nothing in this Agreement provides the Companies, their Personnel, or their agents with any relief from civil liability in an appropriate case.

7.6 **Choice of Law:** This Agreement shall be governed by and interpreted according to the federal laws of the United States.

7.7 **Forum Selection:** Any civil action involving the Companies and the DOJ for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

7.8 **Integrated Agreement:** This Agreement and all appendices hereto is a fully integrated agreement.

7.9 **Statutory and Regulatory References**: All references in this Agreement to statutory and regulatory provisions shall include any future amendments or revisions to such provisions.

7.10 **Amendments**: This Agreement may only be amended by written agreement signed by the Companies and the DOJ.

7.11 **Changes in Circumstances**: If, after the Agreement Modification Date, the DOJ or the Companies believe that changed circumstances warrant a modification or termination of this Agreement (including if the DOJ determines that the terms of this Agreement are inadequate or no longer necessary to address national security concerns), then the Companies shall negotiate in good faith with the DOJ to modify or terminate this Agreement. Rejection of a proposed modification shall not constitute evidence of a failure to negotiate in good faith.

7.13 **Termination**: After this Agreement takes effect, it shall not terminate except upon written notice by the DOJ to the Companies.

7.14 **Severability**: The provisions of this Agreement shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a

court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of such other provision.

7.15 **Waiver**: The DOJ will consider requests for waivers of any provision of this Agreement from the Companies, provided the Companies provide any such requests in writing with an explanation justifying such requests. The decision to grant any such requests shall be within the sole discretion of the DOJ, and no waiver by the DOJ of any provision of, or right under, this Agreement shall be valid unless it is made in writing and expressly provides for the waiver of the specific requirement under a particular provision of this Agreement. Upon reasonable notice to the Domestic Companies and a reasonable opportunity for the Domestic Companies to respond and attempt to address DOJ's concern, the DOJ shall have the right to modify or withdraw any such waiver. The taking of any action by the DOJ or other appropriate governmental authority in the exercise of any remedy shall not be considered a waiver by the DOJ or such authority of any other rights or remedies. The failure of the DOJ to insist on strict performance of any of the provisions of this Agreement, or to exercise any right granted herein, shall not be construed as a relinquishment or future waiver; rather the provision or right shall continue in full force. No waiver by the DOJ of any provision or right shall be valid unless it is in writing and expressly and explicitly provides for the waiver of a specified requirement or requirements under a particular provision or provisions of this Agreement.

7.16 **Counterparts**: This Agreement may be executed in one or more counterparts, including by facsimile, each of which shall together constitute the same instrument.

7.17 **Successors and Assigns**: This Agreement shall inure to the benefit of and shall be binding upon the Companies and all of their respective successors and assigns; for purposes of this Agreement, successors and assigns under this Section 7.17 shall include any corporate name changes. The Companies may not assign any obligations under this Agreement without the prior written consent of the DOJ.

This Agreement is executed on behalf of the Parties:

América Móvil, S.A. de C.V.

By: _____
Name: ALEJANDRO CANTU J.
Title: GENERAL COUNSEL

Date: Nov. 7, 2019

Telecomunicaciones de Puerto Rico, Inc.

By: _____
Name: Enrique Ortiz de Montellano
Title: President & CEO

Date: Nov. 7, 2019

United States Department of Justice

By: _____
Name: David Plotinsky
Title: Principal Deputy Chief

Date: 11/8/19

APPENDIX A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between América Móvil, S.A. de C.V., on behalf of itself and its subsidiaries through which it will hold its interest in Telecomunicaciones de Puerto Rico, Inc., on the one hand, and the U.S. Department of Justice, on the other dated November 7, 2019, which Agreement is intended to enhance the protection of U.S. national security, law enforcement, and public safety. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation.