

NATIONAL SECURITY AGREEMENT

This National Security Agreement (“**Agreement**” or “**NSA**”) is made as of the date of the last signature affixed hereto, (“**Effective Date**”) by and between Altice N.V. (“**Altice**”) and Cequel Corporation (“**Cequel**”), on the one hand, and the U.S. Department of Justice (“**DOJ**”), including the Federal Bureau of Investigation (“**FBI**”), on the other hand (**collectively with all other parties hereto, the “Parties”**).

RECITALS

WHEREAS, United States communication systems are essential to the ability of the United States 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 United States government (“**USG**”) has an obligation to the public to ensure that United States communications and related information are secure in order to protect the privacy of United States persons, to preserve the security of the nation, 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 (see e.g., Executive Order 13,231, Critical Infrastructure Protection in the Information Age, and Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (February 12, 2013));

WHEREAS, the protection of Classified and Sensitive Information also is critical to United States national security;

WHEREAS, Cequel, a Delaware corporation (d/b/a Suddenlink Communications (“**Suddenlink**”)) with its headquarters at 520 Maryville Centre Drive, suite 300, St. Louis, Missouri 63141, currently holds various Federal Communications Commission (“**FCC**”) licenses and authorizations to operate international, domestic, wireless, and cable television relay services (“**CARS**”) in certain markets in the United States and offers a full range of telecommunications and media services to its existing customer base;

WHEREAS, Altice, a Dutch public company, through its subsidiaries, operates as a provider of telecommunications (fixed, mobile) and broadband services in a range of markets throughout the world, including in Western Europe (France, Belgium, Luxemburg, Portugal, and Switzerland), Israel, the French Caribbean and Indian Ocean regions, and the Dominican Republic;

WHEREAS, on May 19, 2015, Altice and Cequel entered into a Purchase and Sale Agreement pursuant to which Altice directly and indirectly will acquire the majority (70.0 percent) of Cequel’s shares;

WHEREAS Altice and Cequel filed a series of applications pursuant to sections 214 and 310(d) of the Communications Act of 1934, as amended, seeking approval for the transfer of control of Cequel and its subsidiaries to Altice;

WHEREAS, more specifically, on June 3, 2015, Altice and Cequel filed applications seeking the FCC's consent to transfer control of Cequel's domestic, international, wireless, and CARS authorities pursuant to the Purchase and Sale Agreement (FCC File Nos. ITC-T/C-20150603-00138 and ITC-T/C-20150603-00139; WC Docket No. 15-135) to Altice in excess of the limitation in 47 U.S.C. § 310(b)(4) regarding foreign ownership (**collectively, the "FCC Applications"**);

WHEREAS, Altice, through its United States subsidiaries, and Cequel have and will continue to have direct physical and electronic access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance, physical search, and storage laws;

WHEREAS, Altice and Cequel, through their United States subsidiaries, have and will continue to have an obligation to protect from unauthorized disclosure the contents of wire and electronic communications to and from the United States under United States law; and

WHEREAS, the DOJ has identified national security, law enforcement, and public safety concerns touching upon issues relating to national security, law enforcement, and public safety that the Parties agree are best addressed through the execution of this Agreement;

NOW, THEREFORE, the Parties enter into this Agreement to address national security, law enforcement, and public safety concerns.

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 internal Altice or Cequel 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 **“Affiliate”** means any entity that Altice controls, as defined in Section 1.9 of this Agreement.
- 1.3 **“Altice”** has the meaning given it in the Recitals, to include any of that entity’s subsidiaries, aside from Cequel itself.
- 1.4 **“Altice U.S. Point of Presence” (“Altice U.S. POP”)** means an Altice or Cequel point of presence in the continental U.S., including U.S. territories, that is subject to the Implementation Plan. Altice U.S. POPs include, but are not be limited to, a site supporting the termination, origination, mediation, routing, and/or switching of Domestic Communication and equipment physically located in the continental and territories of the United States, in such a manner as to provide real-time routing of all Domestic Communications over Altice’s or Cequel’s support of DC in the United States, and meeting all other applicable requirements of this Agreement and the Implementation Plan.
- 1.5 **“Call Associated Data”** means any information relating to a communication or relating to the sender or recipient of that communication and may include, without limitation, subscriber identification, 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.
- 1.6 **“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.
- 1.7 **“Cequel”** has the meaning given it in the Recitals, to include any of that entity’s subsidiaries.
- 1.8 **“Classified Information”** means any information determined pursuant to Executive Order 13,526, as amended or superseded, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.
- 1.9 **“Control” and “Controls”** means the power, direct or indirect, 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 the 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 the entity; or
- (f) Altice's or Cequel's obligations under this Agreement.

1.10 **"Customer Proprietary Network Information ("CPNI")** means:

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

1.11 **"De facto" and "de jure"** control have the meaning provided in 47 C.F.R. § 1.2110, as amended or superseded.

1.12 **"DOJ"** has the meaning given it in the Preamble.

1.13 **"Domestic Communications" (or, "DC")** means:

- (a) Wire Communications or Electronic Communications (whether stored or not) 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) that originates from or terminates at a U.S. location.

1.14 **"Domestic Communications Infrastructure" (or, "DCI")** means:

- (a) the transmission and switching equipment (including hardware, software, and upgrades) used by or on behalf of Altice or Cequel to provide, process, direct, control, supervise or manage Domestic Communications;
- (b) facilities and equipment used by or on behalf of Altice or Cequel that are physically located in the United States; and

- (c) the facilities and equipment used by or on behalf of any Altice or Cequel U.S. subsidiaries to control the equipment or facilities described in (a) and (b) above.
- 1.15 **“Effective Date”** has the meaning given it in the Preamble.
- 1.16 **“Electronic Communication”** has the meaning given it in 18 U.S.C. § 2510(12), as amended or superseded.
- 1.17 **“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, as amended or superseded, and electronic surveillance as defined in 50 U.S.C. § 1801(f), as amended or superseded;
 - (b) Access to or support of stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*, 18 U.S.C. § 2510(17), and 50 U.S.C. § 1821(5), as amended or superseded;
 - (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.*, as amended or superseded;
 - (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), as amended or superseded; and
 - (f) including the Access to, or the acquisition or interception of, communications or information as described in (a) through (e) above, and comparable State laws.
- 1.18 **“FBI”** has the meaning given it in the Recitals.
- 1.19 **“FCC”** has the meaning given it in the Recitals.
- 1.20 **“FCC Applications”** has the meaning given in the Recitals.
- 1.21 **“Foreign”**, where used in this Agreement, whether capitalized or lower case, means non-U.S.
- 1.22 **“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.
- 1.23 **Implementation Plan** means the written blueprint of policies, standards, and procedures that Altice and Cequel will implement in order to comply with this Agreement, subject to the DOJ's approval. Certain of the rights and obligations of the Parties are set forth in further detail in the Implementation Plan, which will be drafted, adopted, and actualized by Altice and Cequel in accordance and consistent with this Agreement pursuant to the Section 2.1 of this NSA. Altice and Cequel shall comply with the Implementation Plan, which may be amended from time to time pursuant to Article VIII.
- 1.24 **"Intercept," "Interception," or "Intercepted"** has the meaning defined in 18 U.S.C. § 2510(4), as amended or superseded.
- 1.25 **"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.
- 1.26 **"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 Domestic Communications, and Call Associated Data, Transactional Data, or Subscriber Information authorized by U.S. law.
- 1.27 **"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 Altice's or Cequel's Domestic Communications Infrastructure: operations and management support; corrective and preventative maintenance including intrusive testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, and development, and the implementation of changes and upgrades.
- 1.28 **"Network Operations Center" or "NOC"** means the locations and facilities designated as such by Altice or Cequel for purposes of performing network management, monitoring, maintenance, provisioning) or other operational functions for Domestic Communications Infrastructure in the U.S. and its territories.
- 1.29 **"Offshore" or "Offshoring"** means, with respect to Domestic Communications, performing obligations of this Agreement through the use of entities and personnel outside the territorial limits of the U.S., whether those entities or personnel are employees of Altice, Cequel, or third parties.

¹ DOCSIS is a standard interface for cable modems.

- 1.30 **“Outsource” or “Outsourcing”** means, with respect to Domestic Communications, supporting the services and operational needs of Altice and Cequel at issue in this Agreement through the use of contractors.
- 1.31 **“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.
- 1.32 **“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.
- 1.33 **“Principal Equipment”** means the primary electronic components of a:
- (a) mobile or fixed communication network;
 - (b) broadband network;
 - (c) transport and fiber network;
 - (d) terrestrial wireless/satellite networks;
 - (e) softswitches;
 - (f) network routers; and
 - (g) call managers/servers.

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.²

- 1.34 **“Screened Personnel”** means those persons described in detail in Article IV, Section 4.13 of this Agreement.
- 1.35 **“Sensitive Information”** means information that is not Classified Information regarding:
- (a) the persons or facilities that are the subjects of Lawful U.S. Process;

² Examples of some Principal Equipment are gateway routers, access routers, home location registers, visitor location registers, smart antennas, software defined radios, call servers, evolved Node B (“eNodeB”), submarine line terminals, optical add-drop multiplexers, mobile switches, circuit switches, Softswitches, private branch exchanges (“PBXs”), microwave radios, etc.

- (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 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."

1.36 **"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, as amended or superseded;
- (b) sought pursuant to the provisions of other Lawful U.S. Process.

1.37 **"Trade Secret"** has the meaning provided in 18 U.S.C. § 1839(3).

1.38 **"Transactional Data"** means:

- (a) any "call identifying information," as defined in 47 U.S.C. § 1001(2), as amended or superseded, including, without limitation, the telephone number or similar identifying designator associated with a communication;³
- (b) Internet address or similar identifying designator associated with a communication;
- (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 Altice and Cequel;
- (e) to the extent associated with a subscriber, user, or account payer of Altice and Cequel, 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

³ Also includes Uniform Resource Locators ("**URLs**") and Internet Protocol ("**IP**") address/header information.

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.
- 1.39 **“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.
- 1.40 **“United States (or U.S.) Law”** means any U.S. federal, state, or local law or regulation.
- 1.41 **“Wire Communication”** has the meaning given it in 18 U.S.C. § 2510(1), as amended or superseded.
- 1.42 **“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**: Altice and Cequel will create an Implementation Plan regarding the methods and processes that will be used to ensure compliance with the NSA, and as outlined and defined in Section 1.23 of this Agreement. Such Implementation Plan is subject to DOJ approval and is due to the DOJ for review within **ninety (90) days** of the Effective Date.
- (a) The Implementation Plan must require Altice and Cequel to prepare network security policy documents subject to DOJ approval for the matters of interest herein; specifically, information security, remote access, physical security, cybersecurity, third-party contractors, outsourcing/offshoring, and Syslogs.
 - (b) 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.
 - (c) The Implementation Plan is deemed adopted once the Parties all agree on its terms and have executed a final copy. The Implementation Plan’s Adoption Date

shall be the date of the last signature affixed thereto. Until such time as the Implementation Plan is adopted, the terms of this NSA shall control.

- 2.2 **Operational Requirements:** With respect to the operation of Altice's and Cequel's Domestic Communications Infrastructure, Altice and Cequel agree as follows, except where otherwise approved by the DOJ:
- (a) **Point of Presence:** Domestic Communications shall be routed through Altice U.S. POPs, or otherwise through a third-party point of presence ("**POP**") in the United States, in accordance with the Implementation Plan (as defined herein) so that, pursuant to Lawful U.S. Process, Electronic Surveillance can be conducted. To the extent that Domestic Communications are routed through an Altice U.S. POP, Altice and Cequel will provide any technical or other assistance required to accomplish such Electronic Surveillance.
 - (b) **Domestic Communications Infrastructure:** All network equipment used for Domestic Communications shall be located in the United States, except as otherwise permitted under the terms of the NSA or policies adopted in accordance therewith. All Domestic Communications Infrastructure shall be managed, directed, controlled, supervised, provisioned, and maintained in accordance with the NSA's terms.
 - (c) **Network Operation Center:** The primary U.S. NOCs supporting any Domestic Communications Infrastructure shall be maintained and remain within the United States and U.S. territories. To operate or support the primary U.S. NOCs, Altice and Cequel shall exclusively rely upon Screened Personnel, as defined herein. Should Altice and Cequel wish to rely upon subcontractors to operate or support the primary U.S. NOCs, such subcontractors will be subject to pre-approval by the DOJ.
 - 1) Within **forty-five (45) days** of the Effective Date, Altice and Cequel shall provide the DOJ with a list of the current subcontractors supporting the U.S. NOCs.
 - (d) **Separation of Domestic Communication and Domestic Communication Infrastructure from Altice:** Altice and Cequel must continue to maintain a network for the U.S. and its territories that is exclusively controlled, managed, and operated from the U.S. and its territories. Any support of DC or DCI relying upon any facility, service, or operation sharing outside the U.S. and its territories must be pre-approved by the DOJ, with the understanding that such facility, service, or operation sharing is subject to the terms of this NSA. Altice and Cequel shall notify the DOJ of such facilities, services, or operation sharing at least **forty-five (45) days** in advance, and the DOJ shall have **forty-five (45) days** after such notice to review and object to the same. Should the DOJ object, the facility, service, or operation sharing at issue will not be actualized; where there is no objection, such facility, service, or operation sharing will otherwise be subject to the terms and strictures of this NSA.

- 2.3 **CPNI**: Altice and Cequel shall comply with all applicable FCC rules and regulations governing Access to and the storage of CPNI.
- 2.4 **Compliance with Lawful U.S. Process**: Altice and Cequel shall take all practicable steps to configure their Domestic Communications Infrastructure such that Altice and Cequel are capable of complying, and Altice and Cequel 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 his/her authority under the Constitution, federal statutes and regulations, and other executive authorities, to include, without limitation, Section 706 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.*).
- 2.5 **Network and Telecommunications Architecture**: Within **sixty (60) days** of the Effective Date, Altice and Cequel shall submit to the DOJ a comprehensive description of their DCI network and detailed transport network diagrams. These descriptions/diagrams shall include the locations of all principal equipment – including core routers, servers, switches, operational systems software, and network security applications and software – as well as architecture interconnect diagrams, architecture flow diagrams, and architecture context diagrams. The comprehensive description also shall include the following information regarding the points of presence, 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 Altice’s and Cequel’s 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;
 - (d) a description of any unique or proprietary application, platform, and or capability that supports the operation of the DCI and/or DC.
- 2.6 **Information Storage and Access**: Altice and Cequel shall make such available in the United States:
- (a) stored Domestic Communications, if such communications are stored by or on behalf of Altice or Cequel for any reason;
 - (b) any Wire Communications or Electronic Communications (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 the account of an Altice or Cequel U.S. user, or routed to an Altice U.S. POP and stored by or on behalf of Altice or Cequel for any reason;

- (c) Transactional Data and Call Associated Data relating to Domestic Communications if such information is stored by or on behalf of Altice or Cequel for any reason;
- (d) billing records relating to Altice or Cequel customers or subscribers for their U.S. operation, Altice customers and subscribers domiciled in the United States, and Altice customers and subscribers who hold themselves out as being domiciled in the United States, as well as billing records related to any call routed through an Altice U.S. POP, if such information is stored by or on behalf of Altice or Cequel 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 Altice or Cequel customers or subscribers for those companies' U.S. operations, including information regarding telecommunications, broadband, wireless, broadcasts, Internet, wireline, video/programming in the United States, and Altice or Cequel customers or subscribers who hold themselves out as being domiciled in the United States, as well as Subscriber Information related to any call routed through an Altice U.S. POP if such information is stored by or on behalf of Altice or Cequel for any reason;
- (f) a description of the placement of NOCs, data centers, and OSS hosting centers;
- (g) a description of Altice's and Cequel's IP/broadband networks and operation processes, procedures for management control, and its 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 Altice and Cequel as well as of Altice's and Cequel's operating and administrative software/platforms.

2.7 **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 2.6, or upon receiving any other preservation request served in compliance with U.S. law, Altice or Cequel 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.

2.8 **Mandatory Destruction**: Altice and Cequel shall ensure that the data and communications described in Section 2.6 of this Agreement are stored in a manner not

subject to mandatory destruction under any foreign laws. Altice shall further ensure that the data and communications described in Section 2.6 of this Agreement shall not be stored by or on behalf of Altice or Cequel outside of the United States.

- 2.9 **Billing Records**: Altice and Cequel 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.
- 2.10 **Compliance with U.S. Law**: Nothing in this Agreement or the Implementation Plan shall excuse Altice or Cequel 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 NON-OBJECTION BY THE GOVERNMENT PARTIES

- 3.1 **Non-Objection to Current Application**: Upon the execution of this Agreement by all of the Parties, the DOJ shall promptly notify the FCC that, provided the FCC conditions the grant of the FCC Applications on Altice's and Cequel's compliance with this Agreement, the DOJ has no objection to the FCC's grant or approval of the FCC Applications. This assurance is given with the understanding that Altice and Cequel will timely submit the Implementation Plan and efficiently address any concerns raised by the DOJ with respect to the content and manifestation of, and compliance with, such Implementation Plan.
- 3.2 **Future Applications**: Nothing in this Agreement or the Implementation Plan shall preclude the DOJ from opposing, formally or informally, any FCC application by Altice to transfer its license(s) to a third party or for 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 IV SECURITY AND SECURE FACILITY

- 4.1 **Location of Secure Facility**: Altice and Cequel shall maintain an appropriately secure facility within the United States within which Altice and Cequel shall:
- (a) take appropriate measures to prevent unauthorized Access to data or facilities that might 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 Altice and Cequel;
 - (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 Section 4.1(b) shall not apply to those non-U.S. citizens already serving in positions handling or regularly dealing with Sensitive Information as part of their job responsibilities as of the Effective Date, so long as the names of all such persons are sent to the DOJ within **sixty (60) days** of the Effective 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 5.10, herein. Once a non-U.S. citizen is notified to the DOJ, should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.1(b).
- 2) If, after the Effective Date, Altice or Cequel deem it necessary to assign a non-U.S. citizen to a position referenced in Section 4.1(b), such party shall seek a waiver from Section 4.1(b)'s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-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 4.1(b). The DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.1(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 by the DOJ. Should the DOJ, within its thirty (30) day objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and Altice or Cequel shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.1(b)(2), the DOJ's thirty (30) day objection period shall be extended by the number of days the DOJ awaited a response from Altice or Cequel.
 - a. Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.1(b) pursuant to Section 4.1(b)(2), the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated pursuant to Section 4.1(b)(1) and submitted to the DOJ in the Annual Report required by Section 5.10 in a manner clearly identifying such persons as appearing on the list by virtue of a waiver. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.1(b)(2), should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.1(b).

- (c) upon the DOJ's request, provide to the DOJ 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 4.5 shall have sufficient authority over any of Altice's or Cequel's 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.

4.2 **Measures to Prevent Improper Use or Access:** Altice shall take all practicable measures to prevent the use of or Access to the equipment or facilities supporting those portions of Altice's and Cequel's DCI's necessary for conducting Electronic Surveillance where such use or Access would violate any U.S. law or 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.

4.3 **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, Altice or Cequel shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to, Domestic Communications, 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, identified representative, or a component or subdivision thereof. Any such requests or submissions of legal process described in this Section 4.3 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 Altice or Cequel, 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. Altice and Cequel shall take reasonable measures to ensure that mechanisms are in place to become aware of all such requests or submission of legal process described in this Section 4.3.

4.4 **Disclosure to Foreign Government Authorities:** Altice 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, 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. Altice and Cequel shall notify the DOJ of any requests or any legal process submitted to Altice or Cequel by a foreign government, identified representative, or a component or subdivision thereof for communications, data, or information identified in this Section 4.4. Altice and Cequel 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 by and known to Altice or Cequel, 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. Altice and Cequel shall take reasonable measures to ensure that they will promptly learn of all such requests or submission of legal process described in this Section 4.4.

- 4.5 **Law Enforcement Points of Contact (“LE POCs”)**: Within **thirty (30) days** after the Effective Date, Altice and Cequel shall designate LE POCs within the United States with the authority and responsibility for accepting and overseeing compliance with Lawful U.S. Process. **Within that same period of time**, Altice and Cequel shall notify the DOJ of the designation of the LE POCs, and include in such notice the PII for the LE POCs.
- (a) Thereafter, Altice and Cequel 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. Altice and Cequel shall cooperate with any request by a government entity within the U.S. 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;
 - 2) any Lawful U.S. Process for Electronic Surveillance, 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.
- 4.6 **Security of Lawful U.S. Process, Sensitive Information, and Classified Information:** Altice and Cequel shall protect the confidentiality and security of all 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. federal and state law or regulations.
- 4.7 **Change in Service Portfolio:** Altice and Cequel agree that they will inform the DOJ at least **30 days in advance** of any material changes to the current-services portfolio for Suddenlink or any successor in interest to Suddenlink, and of offers of other services beyond such portfolio.

- (a) The DOJ enters into this Agreement with the understanding that, as of the Effective Date, such portfolio is no different from that submitted by Cequel and/or Altice in their Team Telecom triage responses electronically received by the DOJ on July 21, October 2, or October 5, 2015.
- (b) Within **ninety (90) days** of the Effective Date, Altice and Cequel will submit to the DOJ a list of their current-offerings/services portfolio, which shall act as the benchmark moving forward regarding the Parties' understandings for obligations under this Agreement.

4.8 **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 Altice's or Cequel's Access to Classified and Sensitive Information.

4.9 **Designation of Security Officer and or Technical Compliance Officer ("SOTCO" or "Security Officer")**: Altice and Cequel 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 Altice or Cequel to perform his/her duties under this Agreement and the Implementation Plan. The SOTCO also shall possess the necessary resources and skills to enforce this Agreement and to act as a liaison to the DOJ regarding compliance with the NSA and the Implementation Plan and to address any national security issues arising in Altice's and Cequel's due course of business. Altice and Cequel shall need to provide the SOTCO with Access to that business information of Altice and Cequel that is necessary for the SOTCO to perform his or her duties.

- (a) Altice and Cequel shall designate its initial SOTCO to the DOJ within **forty-five (45) days** of the Effective 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. Altice and Cequel 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 DOJ review and non-objection, and Altice and Cequel shall reasonably address any concerns raised by the DOJ regarding the selection and identity of the SOTCO.
- (c) With respect to the SOTCO's qualifications, he/she must:
 - 1) be a resident U.S. citizen who possesses U.S. citizenship only (*i.e.*, is not a dual-national);
 - 2) if not already in possession of a U.S. security clearance, shall be eligible, at the sole discretion of the USG, to hold such security clearances immediately upon appointment;
 - 3) be subject to the screening process described in Sections 4.13 and 4.14;

- 4) reside in the continental U.S., in a location that permits and supports the SOTCO's efficient and successful fulfillment of his duties and obligations under the NSA and the Implementation Plan; and
- 5) be a corporate officer with appropriate authority, skills, and resources to enforce this Agreement.

4.10 **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 Altice and Cequel under Section 5.10 of this Agreement;
- (b) Developing and maintaining the Implementation Plan, along with Altice's and Cequel's Information Security Plan (Section 4.11), Access-or-disclosure requirements (described in Sections 4.2, 4.3, and 4.4), Offshoring Control and Access Policy (Section 4.12), personnel-screening-process requirements (described in Sections 4.13 and 4.14), and other policies generally discussed herein (*e.g.*, regarding visitation (Section 4.1(a)) and trade secrets protection (Section 4.16), etc.) to promote full compliance with the 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 the 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 the Agreement;
- (f) Being available upon reasonable notice for discussions with the DOJ relating to the enforcement of and compliance with the Agreement or any other issue involving national security;
- (g) Ensuring procedures are in place for Altice and Cequel to comply with Lawful U.S. Process in an expeditious, effective, and unimpeded fashion; and
- (h) Acting as the liaison with and point of contact for Altice and Cequel for the DOJ.

4.11 **Information Security Plan:** Following the Effective Date, Altice and Cequel 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 pursuant to Section 4.13(a);
- 1) The citizenship limitation of Section 4.11(b) shall not apply to those non-U.S. citizens already serving in positions for which screening is contemplated as of Section 4.13(a) as of the Effective Date, so long as the names of all such persons are sent to the DOJ within **sixty (60) days** of the Effective 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 5.10, herein. Once a non-U.S. citizen is notified to the DOJ, should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.11(b).
 - 2) If, after the Effective Date, Altice or Cequel deem it necessary to assign a non-U.S. citizen to a position referenced in Section 4.11(b), such party shall seek a waiver from Section 4.11(b)'s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-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 4.11(b). The DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.11(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 by the DOJ. Should the DOJ, within its thirty (30) day objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and Altice or Cequel shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.11(b) 2), the DOJ's thirty (30) day objection period shall be extended by the number of days the DOJ awaited a response from Altice or Cequel.
 - a. Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.11(b) pursuant to Section 4.11(b)2), the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated pursuant to Section 4.11(b)1) and submitted to the DOJ in the Annual Report required by Section 5.10 in a manner clearly identifying such persons as appearing on the list by virtue of a waiver. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.11(b)2), should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.11(b).

- (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 the 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 12,968 and 13,467 and other applicable law;
- (f) Ensures that the LE POCs described in Section 4.5 of this Agreement shall have sufficient authority over any employees or contractors of Altice or Cequel 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 and positions that require screening pursuant to this Agreement, the required rigor of such screening by type of position, and the criteria by which Altice will accept or reject Screened Personnel (as defined in Section 4.13);
- (i) Maintains appropriately secure facilities (*e.g.*, offices, communications centers, network operations centers, etc.) within the U.S. for the handling and storage of any Classified Information or Sensitive Information

4.12 Outsourcing and Offshoring Control and Access:

- (a) Altice and Cequel shall not Outsource or Offshore functions covered by this Agreement to an entity that is not within the definition of "Altice" or "Cequel" under this Agreement, except pursuant to the Outsourcing and Offshoring Control and Access Policy adopted pursuant to this NSA and the Implementation Plan, outlined in Section 4.12(b).
 - 1) Where Cequel already is 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 4.12(a), Altice and Cequel shall submit to the DOJ a notice of current outsourcing/offshoring providers within **sixty (60) days** of the Effective Date.

- (b) No later than **ninety (90) days** after the Effective Date, Altice and Cequel will adopt and implement an Outsourcing and Offshoring Control and Access Policy. Altice and Cequel 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 Altice and Cequel to provide the DOJ **forty-five (45) days' prior notice** of any proposed 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.
- 1) All outsourcing and offshoring arrangements shall be subject to Altice's and Cequel's Outsourcing and Offshoring Control and Access Policy, which shall include logical and physical controls (such as restricted access methods and background screening).
 - 2) Altice and Cequel shall not outsource or offshore functions involving DCI, DC, Access to Classified Information, Sensitive Information, or Lawful U.S. Process; and, Altice's and Cequel's Outsourcing and Offshoring Control and Access Policy may not provide for such outsourcing/offshoring.
 - 3) The Outsourcing and Offshoring Control and Access Policy may address classes of outsourcing or offshoring contracts of a routine and nonsensitive nature to be excluded from Section 4.12(b)'s notice-and-approval requirement.

4.13 **Screening of Personnel:** Altice and Cequel shall maintain and implement a screening process to ensure compliance with all personnel-screening-process requirements agreed to herein and in the Implementation Policy. The screening process of Altice and Cequel shall cover any existing or newly hired employees and any personnel performing under an agreement with Altice or Cequel requiring Access/responsibilities in at least the following circumstances:

- (a) All persons who have Access to Classified or Sensitive Information; all persons who have Access to Domestic Communications Infrastructure to monitor the content of Domestic Communications; and all persons who have the ability to monitor personnel with limited access to Domestic Communications under this subsection.
- (b) All persons who have Access to Transactional Data, Subscriber Information, CPNI, CDRs, IPDRs, or PII for customers and network users of Altice and Cequel; all persons who have limited access to Domestic Communications Infrastructure, excluding the ability to monitor the content of Domestic Communications; and all persons who provision network elements either onsite or remotely.

- (c) Nothing in this subsection shall be read to apply the screening requirements in Section 4.13 to Altice/Cequel customers (or their agents) obtaining their own data.

Upon satisfactory completion of the screening-process requirements set forth in this Agreement, such persons shall be considered “**Screened Personnel.**” In addition, Altice and Cequel will cooperate with any reasonable notice by the DOJ to provide additional information necessary for an enhanced background investigation to be conducted by such DOJ with respect to identified Screened Personnel.

4.14 **Screening Process Requirements:** The screening process undertaken pursuant to Sections 4.13 and 4.14 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. Altice and Cequel 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 Effective Date. Thereafter, Altice and Cequel 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) Altice and Cequel shall utilize the criteria identified pursuant to Section 4.13 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) Altice and Cequel shall assign U.S. citizens to positions for which screening is contemplated pursuant to Section 4.13(a).
 - a. The citizenship limitation of Section 4.14(a)1) shall not apply to those non-U.S. citizens already serving in positions handling or regularly dealing with Sensitive Information as part of their job responsibilities as of the Effective Date, so long as the names of all such persons are sent to the DOJ within **sixty (60) days** of the Effective 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 5.10, herein. Once a non-U.S. citizen is notified to the DOJ, should such person leave his/her position, such person’s replacement must comport with the U.S.-citizen requirements of Section 4.13(a)1).
 - b. If, after the Effective Date, Altice or Cequel deems it necessary to assign a non-U.S. citizen to a position referenced in Section 4.14(a)1), such party shall seek a waiver from Section 4.14(a)1)’s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-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 4.14(a)1). The DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.14(a)1)(b) 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 by the DOJ. Should the DOJ, within its thirty (30) day objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and Altice or Cequel shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.14(a)1)b., the DOJ's thirty (30) day objection period shall be extended by the number of days the DOJ awaited a response from Altice or Cequel.

- (i) Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.14(a)1) pursuant to Section 4.14(a)1)b., the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated pursuant to Section 4.14(a)1)a. and submitted to the DOJ in the Annual Report required by Section 5.10 in a manner clearly identifying such persons as appearing on the list by virtue of a waiver. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.14(a)1)b., should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.14(a)1).
- 2) Altice and Cequel may outsource or offshore positions for which screening is contemplated pursuant to Section 4.13(b).
 - a. With respect to outsourced or offshored personnel, Altice and Cequel 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 4.12 of this Agreement.
- 3) Altice and Cequel shall consult with the DOJ regarding the screening procedures to be used and the positions subject to screening. Altice shall reasonably address any concerns the DOJ may raise with respect to such screening procedures. Altice shall use the criteria identified in Section 4.13 of this Agreement to identify the personnel to be screened.

- 4) Altice and Cequel shall cooperate with reasonable requests by the DOJ, or any U.S. Government Authority, desiring to conduct any further background checks.
 - a. 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) Altice and Cequel shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.
 - 6) Altice and Cequel 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 4.14 of this NSA, shall be maintained in a secure and confidential manner strictly in accordance with applicable law.

4.15 **System Security and Integrity (“SSI”)**: Altice and Cequel shall provide the DOJ and the FCC with a current and updated SSI plan within **thirty (30) days** after the FCC’s grant of the Applications, and shall routinely update such SSI plan with the FCC and provide copies of the same to the DOJ.

4.16 **Protection of Trade Secrets**: Altice and Cequel shall affirmatively behave in manners, ways, and means that will demonstrate such entities’ desires to protect and maintain the confidentiality of the trade-secret and proprietary information in their business(es)’ possession(s) to the extent that the safeguarding of such information is necessary to protect Classified Information, Sensitive Information, Subscriber Information, Domestic Communications, DCI, Call Associated Data, CPNI, Transactional Data, and customer PII from inadvertent, unintended, or improper disclosure, or is otherwise relevant to carrying out the provisions of this NSA.

- (a) Within **one hundred and twenty (120) days** of the Implementation Plan’s Adoption Date, Altice and Cequel shall undertake an internal review to determine, in their reasonable discretion, what, if any, Trade Secrets or other proprietary information they possess. Thereafter, Altice and Cequel shall engage in periodic internal reviews to confirm they are adequately identifying their Trade Secret and proprietary information. Such periodic internal reviews shall occur at reasonable intervals for doing so, with no more than **three (3) years** passing between each internal review.
- (b) Should Altice and Cequel, through conducting an internal review of the type described in Section 4.16(a), identify any Trade Secrets or proprietary information, they shall:

- 1) Evaluate the risks to their business(es) presented by the potential for third-party unauthorized access to such Trade Secrets or proprietary information; and
- 2) Take those steps they deem appropriate to mitigate such risks.

ARTICLE V AUDITING, REPORTING AND NOTICE

- 5.1 **Notice of Obligations:** Altice and Cequel shall instruct appropriate officials, 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.
- 5.2 **Reporting of Incidents:** Altice and Cequel shall take all practicable steps under the Implementation Plan to ensure that they shall notify the DOJ if any Altice or Cequel official, employee, contractor, or agent acquires 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 Domestic Communications, 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. federal, state or local law or regulation (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.

Altice's and Cequel's notification shall be made promptly and in any event no later than **ten (10) calendar days** after Altice or Cequel management acquires such information. Further, Altice and Cequel shall lawfully cooperate in investigating the matters pertaining to such notice. Altice and Cequel need not report information where its disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

- 5.3 **Notice of Decision to Store Information Outside the United States:** Altice and Cequel shall provide the DOJ with **thirty (30) days' prior** written notice regarding the storage outside of the U.S. by Altice, Cequel, or any entity with which Altice or Cequel have contracted or made other arrangements for data or communications processing or storage storing of Domestic Communications, Transactional Data, Call Associated Data, Subscriber Information, CDRs, CPNI, or other billing records. 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 Altice or Cequel);
- (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.

5.4 **Notice of Decision to Use Foreign-Located Domestic Communication Infrastructure:**

Altice and Cequel shall provide the DOJ **forty-five (45) days' advance written notice** if Altice or Cequel plans to provide, direct, control, supervise, or manage Domestic Communications through any facilities located outside of the United States and its territories. Upon receipt of such a notice, the DOJ shall have **forty-five (45) days** to object to Altice or Cequel's notified plans. 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 Altice and Cequel to protect DC and DCI.

5.5 **Outsourcing Third Parties:** If Altice or Cequel outsources to third parties any function covered by this Agreement or the Implementation Plan, Altice shall take reasonable steps to ensure that those third parties comply with the applicable terms of this Agreement and Implementation Plan; and, Altice's and Cequel's Outsourcing and Offshoring Control and Access Policy (Section 4.12) shall memorialize this requirement. The reasonable steps that must be taken shall include:

- (a) Altice and Cequel including in the contracts of such third parties, executed on or after the Effective Date (including, for the avoidance of doubt, the subsequent renewal or extension of any contracts with outsourcing third parties with which Altice and/or Cequel have a contract as of the Effective Date), written provisions requiring that such third parties comply with all applicable terms of the Agreement and Implementation Plan;
- (b) Altice and Cequel 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 Altice or Cequel learn that an outsourcing third party or the outsourcing third party's employee has violated a provision of this Agreement or the Implementation Plan, Altice and Cequel **immediately** shall notify the DOJ.
- 1) Upon such notification, and in consultation with the DOJ, Altice and Cequel 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.
- 5.6 **Access to Information:** In response to reasonable requests made by the DOJ, Altice and Cequel shall provide Access to information concerning technical, physical, management, or other security measures and other reasonably available information needed by the DOJ to assess compliance with the terms of this Agreement and the Implementation Plan.
- 5.7 **DOJ Visits and Inspections:** Upon reasonable notice and during reasonable business hours, the DOJ may visit and inspect any part of Altice's and Cequel's Domestic Communications Infrastructure, secure facilities, corporate offices in the United States, and such other facilities that the parties and 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. Altice and Cequel may have appropriate Altice and Cequel employees accompany DOJ representatives throughout any such inspection.
- 5.8 **DOJ Access to Personnel:** Upon reasonable notice from the DOJ, Altice and Cequel will make available for interview officers or employees of Altice, and will seek to require contractors to make available appropriate personnel located in the United States in a position to provide information to verify compliance with this Agreement and the Implementation Plan.
- 5.9 **Approval of Managed Network Service and Principal Equipment Providers:** No later than **thirty (30) days** after the Effective Date, Altice and Cequel 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. Altice and Cequel shall seek approval from the DOJ at least **forty-five (45) days** before using any 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 Altice and Cequel, in which event the DOJ shall be afforded additional time to approve or disapprove any request sent to the DOJ under this Section 5.9. 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 DOJ awaited a response from Altice and/or Cequel or fourteen (14) days after a response from Altice and/or Cequel is received, whichever is greater. Failure by the DOJ to respond within the required timeframe shall be deemed to constitute a non-objection to use.

- (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, Altice or Cequel may utilize the provider or supplier, provided that Altice or Cequel 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. Altice or Cequel may continue to utilize the provider or supplier, provided that the DOJ does not object within **thirty (30) days** of notification to the DOJ, or within the additional time necessary for Altice and/or Cequel to answer DOJ questions, as outlined for the usual process in Section 5.9.
- (b) The emergency authority conferred in Section 5.9(a) may be suspended at will by the DOJ for any length of time deemed necessary by the DOJ should the DOJ conclude that prior emergency action under Section 5.9(a) either did not warrant an emergency or otherwise was not handled appropriately by Altice, Cequel, or the SOTCO. Such suspension by the DOJ must be in writing, and can only be rescinded thereafter by the DOJ in writing. The DOJ shall reasonably and promptly engage with Altice and/or Cequel regarding any suspension of Section 5.9 under this Section 5.9(b).

5.10 **Annual Report:** On or before the yearly anniversary of the Effective Date, a designated senior corporate officer of Altice and/or Cequel shall submit to the DOJ a report assessing Altice's and Cequel's compliance with the terms of this Agreement and the Implementation Plan for the preceding twelve-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) an identification of any material information with respect to this Agreement not specifically identified in this Section 5.10;
- (i) an 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; and
- (j) a list of all non-U.S. 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 4.1(b)1), 4.11(b)1), and 4.14(a)1)a. of this NSA or who need to be added to the list pursuant to Sections 4.1(b)2)a., 4.11(b)2)a., and 4.14(a)1)b.(i) of this NSA.

5.11 **Annual Third-Party Network Security Audit**: Altice and Cequel shall retain and pay for a neutral third party technical engineer or subject matter expert to objectively audit Altice’s and Cequel’s operations and compliance with this NSA every two years, provided that the DOJ may request that Altice and Cequel 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, the DOJ will make every attempt 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 year** from the Implementation Plan’s Adoption Date, with the final reports for each subsequent audit due every **two years** thereafter (*e.g.*, the second final audit report would be due three years after the Implementation Plan’s Adoption 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 5.11 at the end of the relevant two-year period between standard audits, unless otherwise waived by the DOJ.
- (b) Altice and Cequel shall provide notice of, and terms of reference for, their selected auditor to the DOJ, and the DOJ 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, Altice and Cequel shall work in good faith to resolve such objection.
- (c) Altice and Cequel 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 the DOJ commenting on an audit’s terms, Altice and Cequel shall work in good faith to resolve the DOJ’s comments and requests changes and/or insertions by the DOJ.

- (d) Through their contract with the selected auditor, Altice and Cequel 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) Development of an initial vulnerability and risk assessment based on this Agreement, and a detailed audit work plan based on such assessment.
 - 2) Authority for the auditor to review and analyze Altice and Cequel's security policies and procedures related to network security, methods for protecting the companies' trade secrets touching upon the matters addressed in this Agreement, and those policies discussed in this NSA;
 - 3) Authority to audit the integrity of password systems, review access logs, Syslogs, and review logs regarding any access to a capacity to conduct Electronic Surveillance;
 - 4) Authority for the Auditor to reports, summaries, and other information regarding Altice's and Cequel's efforts to monitor network devices via logs and active polls for unauthorized access or access above assigned privileges, including to U.S. Records, and to include any known security issues;
 - 5) Authority for the auditor to conduct a reasonable number of unannounced inspections of Altice's and Cequel's facilities; and
 - 6) Authority for the auditor to conduct a reasonable volume of random testing of network firewalls, access points, and other systems for potential vulnerabilities.
- 5.12 **Network Changes**: Altice and Cequel 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**.
- 5.13 **Control of Altice/Cequel**: Altice and Cequel 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 Altice or Cequel, except for filings with the FCC for assignments or transfers of control to any U.S. subsidiary of Altice that are *pro forma*.
- 5.14 **Corporate Restructuring**: Altice and Cequel shall **promptly** notify the DOJ of any corporate restructuring of Altice and/or Cequel.
- 5.15 **Notices**: All communications or other notices relating to this Agreement or the Implementation Plan may 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 the NSA. All communications or other notices relating to this Agreement or the Implementation Plan shall be deemed given:

- (a) when delivered personally;
- (b) if by e-mail, as of the electronic time stamp in the DOJ's e-mail account(s);
- (c) if by facsimile, upon transmission with confirmation of receipt by the receiving party's facsimile terminal;
- (d) if sent by documented overnight courier service, on the date delivered; or
- (e) 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:

For the DOJ:

U.S. Department of Justice
Assistant Attorney General for National Security
Attn: Director, Foreign Investment Review Staff
600 E St. NW, 10th Floor
Washington, DC 20004

For Altice:

Altice N.V.
Prins Bernhardplein 200
1097 JB Amsterdam
The Netherlands
Attn: Alexandre Marque, General Counsel
Email: alexandre.marque@altice.net

With a copy to:

David N. Fagan
Covington & Burling LLP
One City Center
850 Tenth St. NW
Washington, DC 20001

For Cequel:

Cequel Corporation
520 Maryville Centre Drive
Suite 300

St. Louis, MO 63141
Tel: 314.315.9400
Attn: General Counsel

ARTICLE VI FREEDOM OF INFORMATION ACT

- 6.1 **Protection from Disclosure:** The DOJ shall take all reasonable measures to protect from public disclosure all information submitted by Altice and Cequel to the DOJ in connection with this Agreement and clearly marked with the legend:

“Confidential; Subject to Protection Under 5 U.S.C. Section 552(b); Not to be Released Without Notice to Altice,” or similar designation.

Such markings shall signify that it is Altice’s or Cequel’s position that the information so marked constitutes “trade secrets” and/or “commercial or financial information obtained from a person and privileged or confidential,” or otherwise warrants protection within the meaning of 5 U.S.C. § 552(b)(4). If a request is made under 5 U.S.C. § 552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, the DOJ, as appropriate, shall notify Altice and/or Cequel of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 25, 1987). If Altice or Cequel objects to the intended disclosure and its objections are not sustained, the DOJ, as appropriate, shall notify Altice of its intention to release (as provided by Section 5 of Executive Order 12600) not later than **five (5) business days** prior to disclosure of the challenged information.

- 6.2 **Use of Information for U.S. Government Purposes:** Nothing in this Agreement or the Implementation Plan shall prevent the DOJ from lawfully disseminating information as appropriate to seek enforcement of this Agreement or the Implementation Plan, provided that the DOJ takes all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

ARTICLE VII OTHER

- 7.1 **Informal Resolution:** The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement or the Implementation Plan. Disagreements shall be addressed by the Parties, in the first instance, at the staff level by their designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to higher authorized officials, unless the DOJ believes that important U.S. interests can be protected, or the Parties believe that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 7.2 below. If, after meeting with higher authorized officials, any Party determines that further negotiations would be fruitless, then any Party may resort to the remedies set forth in Section 7.2 below. If resolution of a disagreement requires Access

to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances.

- 7.2 **Enforcement of Agreement and the Implementation Plan:** Subject to Section 7.1 of this Agreement, if any Party believes that any other Party has breached or is about to breach this Agreement or the Implementation Plan, that Party may bring an action against the other Party for appropriate judicial relief. Subject to Article III and Section 7.1, nothing in this Agreement or the Implementation Plan shall limit or affect the right of the DOJ or a U.S. Government Authority to:
- (a) seek revocation by the FCC of any license, permit, or other authorization granted or given by the FCC to Altice or Cequel, or seek any other action by the FCC regarding Altice or Cequel; or
 - (b) seek civil sanctions for any violation of any U.S. law or regulation or term of this Agreement or the Implementation Plan; or
 - (c) pursue criminal sanctions against Altice or Cequel or any of its respective directors, officers, employees, representatives or agents, or against any other person or entity, for violations of the criminal laws of the United States.
- 7.3 **Forum Selection:** Any civil action for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement or the Implementation Plan shall be brought, if at all, in the United States District Court for the District of Columbia.
- 7.4 **Irreparable Injury:** Altice and Cequel agree that the United States would suffer irreparable injury if for any reason Altice or Cequel failed to perform any of their significant obligations under this Agreement or the Implementation Plan, and that monetary relief would not be an adequate remedy. Accordingly, Altice and Cequel agree that, in seeking to enforce this Agreement or the Implementation Plan, the DOJ shall be entitled, in addition to any other remedy available at law or equity and pursuant to a valid court order, to specific performance and injunctive or other equitable relief.

ARTICLE VIII DISPUTES, AND MISCELLANEOUS

- 8.1 **Right to Make and Perform Agreement:** Altice and Cequel represent that they have and shall continue to have throughout the term of this Agreement and the Implementation Plan the full right to enter into this Agreement and the Implementation Plan, and to perform their obligations hereunder, and that this Agreement and the Implementation Plan are legal, valid, and binding obligations enforceable in accordance with their terms.
- 8.2 **Non-Relinquishment of Rights:** The availability of any civil remedy under this Agreement or the Implementation Plan shall not prejudice the exercise of any other civil remedy under this Agreement, the Implementation Plan, or under any provision of law,

nor shall any action taken by a Party in the exercise of any remedy be considered a waiver by that Party of any other rights or remedies. The failure of any Party to insist on strict performance of any of the provisions of this Agreement or the Implementation Plan, or to exercise any right they grant, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by any Party of any provision or right shall be valid unless it is in writing and signed by the Party, and shall impact the rights of such party to retract, void, or terminate such waiver unless such a right is granted in a waiver.

- 8.3 **Headings**: The article and section headings and numbering in this Agreement and the Implementation Plan are inserted for convenience only and shall not affect the meaning or interpretation of this Agreement or the Implementation Plan.
- 8.4 **Other Laws**: Nothing in this Agreement or the Implementation Plan is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local law or regulation on the Parties; (b) any enforcement authority available under any U.S. federal, state or local law or regulation; (c) the sovereign immunity of the United States; or (d) any authority that the DOJ may possess over Altice's or Cequel's activities or facilities wherever located.
- 8.5 **Statutory References**: All references in this Agreement to statutory provisions shall include any future amendments or superseding replacements to such statutory provisions.
- 8.6 **Non-Parties**: Nothing in this Agreement or the Implementation Plan is intended to confer, or does confer, any rights or obligations on any Person other than the Parties and any other Governmental Authority in the United States authorized to effect Electronic Surveillance pursuant to Lawful U.S. Process.
- 8.7 **Modification**: This Agreement and the Implementation Plan may only be modified by written agreement signed by all of the Parties. Any substantial modification to this Agreement shall be reported to the FCC within **thirty (30) days** of the date of the last signature affixed to a written modification of the Agreement by the Parties.
- 8.8 **Waiver**: Either Party may seek individual waivers from specific terms, obligations, or portions of this Agreement by requesting such waiver from the other Parties. Waivers from specific terms, obligations, or portions of this Agreement must be granted in writing to be effective, and can be subject to terms and conditions imposed, or withdrawn at any time, by the granting Party.
- 8.9 **Partial Invalidity**: If any portion of this Agreement or the Implementation Plan is declared invalid by a U.S. court of competent jurisdiction, or by subsequent events affecting the corporate structure of Altice or Cequel, this Agreement and the Implementation Plan shall be construed as if such portion had never existed, unless such construction would constitute a substantial deviation from the Parties' intent as reflected in this Agreement.
- 8.10 **Good Faith Negotiations**: The DOJ agrees to negotiate in good faith and promptly with respect to any request by Altice or Cequel for modification of this Agreement if the

obligations imposed on Altice or Cequel under this Agreement become unduly burdensome to Altice or Cequel or adversely affect Altice's or Cequel's competitive position, or are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, or public safety concerns. If the DOJ finds that the terms of this Agreement or the Implementation Plan are inadequate to address national security, law enforcement, and public safety concerns presented by an acquisition by Altice or Cequel in the United States after the date that all the Parties have executed this Agreement, Altice shall negotiate in good faith to modify this Agreement or the Implementation Plan to address those concerns.

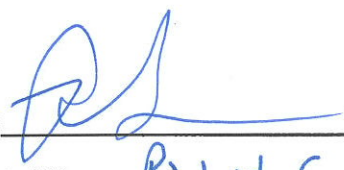
- 8.11 **Successors and Assigns:** This Agreement and the Implementation Plan shall inure to the benefit of, and shall be binding upon Altice, Cequel, the DOJ, and their respective successors and assigns. This Agreement and the Implementation Plan shall apply in full force and effect to any entity or asset, whether acquired before or after the Effective Date, over which Altice and Cequel, including its successors or assigns, has the power or authority to exercise *de facto* or *de jure* control.
- 8.12 **Joint Ventures:** Altice and Cequel have entered into or may enter into joint ventures or other arrangements under which a joint venture or another entity may provide Domestic Communications services. If Altice or Cequel have the power or authority to exercise *de facto* or *de jure* control over such entity, then Altice or Cequel will ensure that such entity shall fully comply with the terms of this Agreement and the Implementation Plan. To the extent that Altice or Cequel lacks such power or authority over such an entity, Altice or Cequel shall in good faith endeavor to have such entity comply with this Agreement and the Implementation Plan and shall consult with the DOJ about the activities of such entity.
- 8.13 **Effective Date of Agreement:** Except as otherwise specifically provided in the provisions of this Agreement, the obligations imposed and the rights conferred by this Agreement shall take effect upon the Effective Date.
- 8.14 **Termination of Agreement:** This Agreement may be terminated at any time by a written agreement signed by the Parties. The Parties agree that they will reasonably consider any termination request submitted pursuant to this Agreement.
- 8.15 **Counterparts:** This Agreement may be executed in one or more counterparts, including by facsimile or portable document format ("**PDF**"), each of which shall together constitute one and the same agreement.

EXECUTION

This Agreement is executed on behalf of the Parties:

United States Department of Justice

Date: 12/11/15

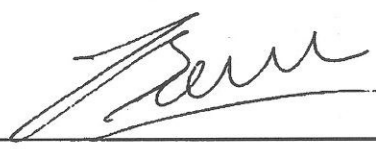
By: 

Printed Name: Richard C. Sofield

Title: Director, Foreign Investment Review Staff

Altice, N.V.

Date: December 11, 2015

By: 

Printed Name: Jérémie BONNIN

Title: General Secretary

Cequel Corporation

Date: _____

By: _____

Printed Name: _____

Title: _____

EXECUTION

This Agreement is executed on behalf of the Parties:

United States Department of Justice

Date: _____

By: _____

Printed Name: _____

Title: _____

Altice, N.V.

Date: _____

By: _____

Printed Name: _____

Title: _____

Cequel Corporation

Date: 12/11/15

By: 

Printed Name: Craig L Rosenthal

Title: Senior Vice President & General Counsel