FISHMAN
ADVISORS PLLC
400 Central Park West 3R, New York, New York 10025 tel 240-475-0620

September 23, 2014

Via IBFS

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

Re: Global Caribbean Network SAS
File Nos. ITC-214-20050623-00237, ITC-214-20050621-00231, and SCL-LIC-20050418-00010
Modification of License Request

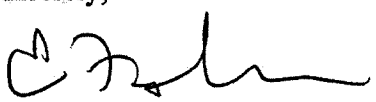
Dear Ms. Dortch:

By its attorney, Global Caribbean Network SAS ("GCN") hereby reports to the Commission that, effective September 8, 2014, together with its parent companies Global Caribbean Fiber SAS ("GCF") and Auto-Guadeloupe Investissement, S.A. ("AGI") (collectively, the "Loret Companies"), it entered into the attached Network Security Agreement with the U.S. Department of Homeland Security and the U.S. Department of Justice (the "U.S. Government Parties"). GCN requests that the Commission condition GCN's above-captioned authorizations upon the compliance by the Loret Companies to the terms of the Network Security Agreement.

Background. The Loret Companies entered into the Network Security Agreement at the request of the U.S. Government Parties in connection with their review of the application for transfer of control of Antilles Crossing – St. Croix, Inc. ("ACSC") from GCF to Fiber Investment Holdings Limited IBC ("FIHL"). By Public Notice, DA 14-1311, released September 10, 2014, the Commission announced its grant of that application subject to the compliance by ACSC and FIHL to the terms of the December 7, 2007 Agreement by and among ACSC, Leucadia National Corporation and AGI, as amended by the September 8, 2014 Amendment No. 1 to the December 7, 2007 Agreement. See SCL-T/C-20131219-00017. In conjunction with their review of the ACSC transfer of control application, the U.S. Government Parties also requested the Loret Companies to enter into a separate Network Security Agreement governing the GCN submarine fiber optic network, and that the above-captioned GCN authorizations be conditioned upon compliance by the Loret Companies with the terms of the Network Security Agreement.

Please direct any questions regarding this matter to the undersigned counsel.

Sincerely,



Eric Fishman
Counsel to Global Caribbean Network SAS
Global Caribbean Fiber SAS and
Auto-Guadeloupe Investissement, S.A.

Enclosure

cc: David Krech, International Bureau
david.krech@fcc.gov

Department of Justice
Assistant Attorney General
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530
ttelecom@usdoj.gov

Department of Homeland Security
Assistant Secretary
Office of Policy
C/O Director, Foreign Investment Risk Management
245 Murray Lane, SW
Mail Stop: 0445
Washington, D.C. 20528
ip-fcc@hq.dhs.gov

Network Security Agreement

THIS NETWORK SECURITY AGREEMENT (the "NSA") is made as of the date of the last signature affixed hereto, by and between Global Caribbean Network SAS ("GCN"), Global Caribbean Fiber SAS ("GCF"), and Auto-Guadeloupe Investissement, S.A. ("AGI"), on the one hand, and the U.S. Department of Justice ("DOJ") and the U.S. Department of Homeland Security ("DHS") (referred to collectively as the "USG Parties"), on the other (referred to individually as a "Party" and collectively as the "Parties"), hereby agree as follows:

Recitals

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

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

WHEREAS, it is critical to the well being of the Nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (see e.g., Executive Order 13231, Critical Infrastructure Protection in the Information Age, and Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience (February 12, 2013));

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

WHEREAS, GCN is a French company that owns and operates a fiber-optic submarine cable network licensed by the Federal Communications Commission ("FCC") to provide non-common carrier service between Puerto Rico, Guadeloupe, St. Martin and St. Croix, and common carrier service between Puerto Rico and St. Barthelemy;

WHEREAS, GCN is a wholly owned subsidiary of GCF, a French company which owns and operates fiber-optic submarine cable networks in the Caribbean by and through its following subsidiaries: Global Caribbean Network ("GCN"), Middle Caribbean Network ("MCN") and Southern Caribbean Fiber ("SCF"), and Antilles Crossing – St. Croix, Inc. ("ACSC");

WHEREAS, GCF is presently jointly owned by (a) Auto-Guadeloupe Investissement S.A. d/b/a Loret Group, a private limited company organized under the laws of France, and Outre-Mer Numerique Holding SAS, an entity organized under the laws of France and a wholly owned AGI subsidiary (60% in the aggregate), and (b) Caribbean Fiber Holdings, LP, a wholly owned subsidiary of Leucadia National Corporation (40%);

WHEREAS, on September 13, 2005, the FCC granted to GCN a submarine cable landing license pursuant to the Cable Landing License Act of 1921[1] and Executive Order No. 10530[2], FCC File No. SCL-LIC-20050418-00010;

WHEREAS, ACSC, Leucadia, and AGI on the one hand, and DOJ and DHS, on the other, entered into an agreement dated as of December 16, 2007 (the "2007 Agreement"), with respect to the transfer of ownership of ACSC from Leucadia to GCF, and which, by its terms, applied to equipment, facilities, and services pertaining to any cable system owned or controlled by ACSC, Leucadia, or AGI, to include those owned or controlled by GCN;

WHEREAS, Leucadia has agreed to sell to GCF, and GCF has agreed to purchase, Leucadia's 40% share in GCF, thereby fully terminating any direct or indirect ownership stake by Leucadia in GCF, GCN, and ACSC;

WHEREAS, GCF, and certain of its affiliates, have entered into a Share and Asset Purchase Agreement with Fibre Investments Holding Limited IBC ("FIHL"), a newly formed company organized under the laws of St. Lucia, and Digicel Investments France SAS ("DIF"), a newly formed company organized under the laws of France and an affiliate of FIHL, pursuant the terms of which GCF has agreed to sell to FIHL all of GCF's shares in ACSC and in AC (Barbados) IBC, the parent of Antilles Crossing (St. Lucia) Limited (AC St. Lucia), and GCF has agreed to sell to DIF a 99.99% interest in AC Barbados LP (ACBLP) and a 99.99% interest in Antilles Crossing International, LP (ACI);

WHEREAS, AGI will retain ownership of GCF and GCN, and DIF and FIHL will not own any interest in AGI, GCF, or GCN;

WHEREAS, GCN provides electronic communication services including telephone services to and from the U.S., which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, GCN has direct physical and electronic access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

WHEREAS, GCN has an obligation to protect from unauthorized disclosure the contents of wire and electronic communications to and from the U.S. under U.S. laws;

WHEREAS, DHS and DOJ have agreed to modify the 2007 Agreement to terminate any obligations of AGI, GCN or GCF under such agreement upon consummation of the transactions described herein, and subject to the conclusion of this NSA;

WHEREAS, DHS and DOJ will request that the FCC's 2005 grant of the authority to GCN, FCC File No. SCL-LIC-20050418-00010, be made subject to resolution of issues relating to national security, law enforcement, and public safety as they relate to the GCN network, and

[1] Pub. Law No. 8, 67 Congress, 42 Stat. 8 (1921); 47 U.S.C. §§ 34-39.

[2] Exec. Ord. No. 10530 § 5 (a) (May 10, 1954), reprinted as amended in 3 U.S.C. § 301.

whereas GCN, GCF and AGI have agreed to enter into this NSA with DHS and DOJ to address issues raised by DHS and DOJ, and to jointly petition that the FCC condition cable landing license SCL-LIC-20050418-00010 (September 13, 2005) on compliance with this NSA;

NOW THEREFORE, the Parties are entering into this NSA to address national security, law enforcement and public safety concerns.

ARTICLE 1: DEFINITION OF TERMS

As used in this NSA:

1.1 "**Applicant-Parties**" means GCN, GCF and AGI.

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

1.3 "**Affiliate**" means any entity that any of the Applicant-Parties owns or Controls.

1.4 "**Cable System**" means all equipment, facilities and services pertaining to any cable system owned or Controlled by any of the Applicant-Parties or their Affiliates, and all network operations centers ("NOCs").

1.5 "**Classified Information**" shall have the meaning indicated in Executive Order 12958, as amended by Executive Order 13292, or any successor executive order, or the Atomic Energy Act of 1954d, or any statute that succeeds or amends the Atomic Energy Act of 1954.

1.6 "**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 with respect to the matters described in Sections 1.7(a) through (d); or

(f) the Applicant-Parties' obligations under this NSA.

1.7 "**De facto**" and "**de jure**" control have the meanings provider in 47 C.F.R. § 1.2110.

1.8 "**Domestic Communications**" means: (a) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location, and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States.

1.9 "**Domestic Communications Infrastructure**" means any portion of the Cable System used by or on behalf of the Applicant-Parties or their Affiliates that is: (a) transmission, switching, bridging and routing equipment (including software and upgrades) to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment physically located in the United States; and (c) facilities to control the equipment described in (a) and (b) above, but does not include entities with which the Applicant-Parties or their Affiliates have contracted for peering, interconnection, roaming, long distance or other similar arrangements on which the Parties may agree, nor equipment or facilities used by service providers other than the Applicant-Parties or their Affiliates that are:

(1) interconnecting communications providers; or

(2) providers of services or content that are:

(A) accessible using the communications services of the Applicant-Parties or their Affiliates, and

(B) available in substantially similar form and on commercially reasonable terms through communications services of companies other than the Applicant-Parties or their Affiliates.

1.10 "**Effective Date**" means the date this NSA becomes effective, which is the date this NSA is signed by the last Party to sign it (as indicated by the date stated opposite that Party's signature).

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

1.12 "**Electronic Surveillance**" for the purposes of this NSA includes: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.; (c) acquisition of dialing routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.; (d) acquisition of location-related information concerning a service subscriber or

facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) Access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

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

1.14 "**Government**," "**Government Authority**," or "**Government Authorities**" means any government, or any governmental, administrative, or regulatory entity, commission, board, agency, instrumentality, bureau or political subdivision and any court, tribunal, judicial or arbitral body.

1.15 "**Intercept**" or "**Intercepted**" has the meaning defined in 18 U.S.C. § 2310(4).

1.16 "**Lawful U.S. Process**" means lawful U.S. federal, state, or local Electronic Surveillance or other court orders, processes, or authorizations issued under U.S. federal, state, or local law for physical search or seizure, production of tangible things, or Access to or disclosure of Domestic Communications, Transactional Data, or Subscriber Information.

1.17 "**Management of the Applicant-Parties**" means their officers and members of the Board of Directors.

1.18 "**Network Management Information**" means network management operations plans, processes and procedures; descriptions of the placement of Network Operating Center(s) and linkages (for service offload or administrative activities) to other domestic and international carriers, ISPs and other critical infrastructures; descriptions of networks and operations processes and procedures for management control and relation to the backbone infrastructure(s) including other service providers description of any unique or proprietary control mechanisms as well as operating and administrative software; and network performance information.

1.19 "**Pro forma assignments**" or "**pro forma transfers of control**" are transfers that do not involve a substantial change in ownership or control as provided by Section 3.24 of the FCC's Rules 947 C.F.R. § 63.24).

1.20 "**Sensitive Information**" means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process; (b) the identity of the Government Authority or Government Authorities serving such Lawful U.S. Process; (c) the location or identify of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance; (d) the means of carrying out Electronic Surveillance; or (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process as well as all other information that is not Classified Information but is designated in writing by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information" of some type recognized by the agency involved. The designation "Sensitive" as used in this Section includes but is not limited to information marked or labeled "Official Use Only," "Limited Official Use Only,"

"Law Enforcement Sensitive," "Sensitive Security Information," "Sensitive but Unclassified," "Controlled Unclassified Information" or other similar designation.

1.21 **"Subscriber Information"** means all records or other information relating to customers or subscribers of the Applicant-Parties or their Affiliates of the type referred to and Accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.

1.22 "**Transactional Data**" includes the following when associated with a Domestic Communication but does not include the content of any communication:

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

(b) any information related to the sender or recipient of that Domestic Communication, including, without limitation, subscriber identification, called party number, calling party number, start time, and time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party members, post-cut-through dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold;

(c) any information relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers domain names, Internet Protocol ("IP") addresses, Uniform Resource Locators ("URLs"), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (e) below.

(d) The time, date, size, or volume of data transfers, duration, domain names, Media Access Control ("MAC") or IP addresses (including source and destination), URL's, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics, including electronic mail headers showing From: and To: addresses; and

(e) As to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.

1.23 "**United States**," "**US**," or "**U.S.**" means the United States of America, including all of its States, districts, territories, possessions, commonwealths, and the special maritime and territorial jurisdiction of the United States.

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

1.25 **Other Definitional Provisions**. Other capitalized terms used in this NSA and not defined in this Article shall have the meanings assigned them elsewhere in this NSA. The definitions in this NSA are applicable to the singular as well as the plural forms of such terms and to the masculine as well as to the feminine and neuter genders of such term. Whenever the words "include," "includes," or "including" are used in this NSA, they shall be deemed to be followed by the words "without limitation."

ARTICLE 2: FACILITIES, INFORMATION STORAGE AND ACCESS

2.1 **Compliance with Lawful U.S. Process**. The Applicant-Parties and their Affiliates shall configure their Domestic Communications Infrastructure to be capable of complying, and the employees of the Applicant-Parties and their Affiliates in the United States will have unconstrained authority to comply in an effective, efficient and unimpeded fashion, with:

(a) Lawful U.S. Process;

(b) the orders of the President of the United States in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended (47 U.S.C. § 606), and under § 302 of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382); and

(c) 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.).

2.2 **Information Storage**. Unless otherwise agreed to by the Parties, the Applicant-Parties shall make the following available in the United States:

(a) stored Domestic Communications, if such communications are stored by or on behalf of the Applicant-Parties for any reason;

(b) any Wire Communications or Electronic Communications received by, intended to be received by, or stored in the account of a domestic customer or subscriber of the Applicant-Parties or their Affiliates, if such communications are stored by or on behalf of the Applicant-Parties or their Affiliates for any reason;

(c) Transactional Data, if such data are stored by or on behalf of the Applicant-Parties or their Affiliates for any reason;

(d) Subscriber Information, if such information is stored by or on behalf of the Applicant-Parties or their Affiliates for any reason;

(e) Billing records of customers or subscribers, if such information is stored by or on behalf of the Applicant-Parties or their Affiliates for any reason; and

(f) Network Management Information.

Nothing in this Section is meant to exclude the use of Transactional Data for business or network management purposes in the normal course of business if said data is subject to security and Access controls. The phrase "on behalf of" as used in this Section does not include entities with which the Applicant-Parties or their Affiliates has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

2.3 **Storage Pursuant to 18 U.S.C. § 2703(f)**. Upon a request made pursuant to 18 U.S.C § 2703(f) by a Government Authority within the United States to preserve any information in the possession, custody, or control of the Applicant-Parties or their Affiliate, including any information that is listed in Section 2.2 above, the Applicant-Parties shall ensure such preserved records or other evidence is stored in the United States.

2.4 **Compliance with U.S. Law**. Nothing in this NSA shall excuse the Applicant-Parties or their Affiliates from any obligation they may have to comply with U.S. legal requirements for the retention, preservation, or production of information, records or data as well as all applicable requirements of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, et seq.

2.5. **Storage of Protected Information**. The Applicant-Parties shall ensure that GCN, GCF and AGI store all Classified Information and Sensitive Information in the United States.

2.6 **List of Principal Equipment**. Within sixty (60) days of the execution of this NSA, and thereafter as part of the Annual Report required pursuant to Section 5.8 of this NSA, Applicant-Parties shall provide the Government Parties an updated list of Principal Equipment. For purposes of this NSA, "Principal Equipment" means the primary components of the Domestic Communications Infrastructure, including, but not limited to, should they exist, servers, routers, switches, signal modulators and amplifiers, repeaters, submarine line terminal equipment (SLTE), system supervisory equipment (SSE), power feed equipment (PFE), tilt and shape equalizer units (TEQ/SEQ), optical distribution frames (ODF), and synchronousoptical network (SONET), synchronous digital hierarchy (SDH), wave division multiplexing (WDM), dense wave division multiplexing (DWDM), coarse wave division multiplexing (CWDM) or optical carrier network (OCN) equipment, as applicable, and any non-embedded software necessary for proper monitoring, administration and provisioning. The list should include all available information on each item's manufacturer and the model and/or version number of any hardware or software. In addition, the list should identify any vendors, contractors, or subcontractors for the Principal Equipment, including those performing functions that would otherwise be performed by Applicant-Parties personnel to install, operate, manage, or maintain the Principal Equipment. Applicant-Parties shall discuss in good faith with the Government Parties any national security, law enforcement or public safety concerns raised by the Government Parties regarding Principal Equipment.

ARTICLE 3: SECURITY

3.1 **Measures to Prevent Improper Use or Access**. The Applicant Parties and their Affiliates shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or the Access, obtain or disclose Domestic Communications, Transactional Data, Subscriber Information, Classified Information or Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this NSA. The Applicant-Parties shall submit the policies and procedures regarding these measures to the DHS and DOJ within ninety (90) days of the effective date for review. The company agrees to meet and confer with the DHS and DOJ and reasonably address any concerns they may have about the policies or the procedures described therein.

3.2 **Access by Foreign Government Authorities**. The Applicant-Parties and their Affiliates shall not directly or indirectly, disclose or permit disclosure of, or provide Access to Domestic Communications, Transactional Data, or Subscriber Information, stored by or on behalf of the Applicant-Parties or their Affiliates to any person if the purpose of such Access is to respond to the legal process or the request of or on behalf of a Foreign Government, identified representative, component or subdivision thereof, without the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States. Any such requests or submissions of legal process shall b reported to DHS and DOJ as soon as possible and in no event later than ten (10) business days after such request or legal process is received by or known to the Applicant-Parties or their Affiliates. The Applicant-Parties and their Affiliates shall take reasonable measures to ensure that it will promptly learn of such requests or submission of legal process.

3.3 **Disclosure to Foreign Government Authorities.** The Applicant Parties and their Affiliates shall not directly or indirectly disclose or permit disclosure of, or provide Access to:

(a) Classified or Sensitive Information;

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

(c) the existence of Lawful U.S. Process that is not already a matter of public record

to any Foreign Government, identified representative, component or subdivision thereof, without satisfying all applicable U.S. federal, state and local legal requirements, and without obtaining either the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States. Any requests of any legal process submitted by a Foreign Government, an identified representative, a component or subdivision thereof to the Applicant-Parties for the communications, data or information identified that is maintained by the Applicant-Parties shall be referred to DHS and DOJ as soon as possible and in no event later than ten (10) business days after such request or legal process is received by or known to the

Applicant-Parties or their Affiliates, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. The Applicant-Parties shall take reasonable measures to ensure that they will promptly learn of all such requests or submissions of legal process.

3.4 **Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities**. Within ten (10) business days after receiving legal process or requests from Foreign non-governmental entities for Access to or disclosure of Domestic Communications, the Applicant-Parties shall notify DHS and DOJ in writing of such legal process or requests, unless such disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

3.5 **Security of Lawful U.S. Process**. The Applicant-Parties and their Affiliates shall protect the confidentiality and security of all Lawful U.S. Process served upon it and the confidentiality and security of Classified and Sensitive Information in accordance with U.S. federal and state law or regulation and this NSA.

3.6 **Point of Contact**. Within ten (10) business days after the Effective Date, the Applicant-Parties shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to its customers or subscribers. The points of contact shall be in the United States, shall 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 Classified Information, Sensitive Information and any Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure or relating the GCN's customers or subscribers. Within ten (10) business days after designating such points of contact, the Applicant-Parties shall notify DHS and DOJ of any change in such designation, also within ten (10) business days. The points of contact shall be resident U.S. citizens who, based on the information in the Applicant-Parties' possession, are eligible for appropriate U.S. security clearances. The Applicant-Parties shall cooperate with any request by a Government Authority within the United States that a background check, security clearance or both be completed for a designated point of contact.

3.7 **Information Security Plan**. The Applicant-Parties shall:

(a) take appropriate measures to prevent unauthorized Access to data or facilities that might contain Classified or Sensitive Information;

(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 person as Sensitive Information;

(c) upon request from DHS or DOJ, provide the name, date of birth, and other relevant identifier information of each person who regularly handles or deals with Sensitive Information;

(d) require that personnel handling Classified Information shall have been granted appropriate security clearances pursuant too Executive Order 12968;

(e) provide that the points of contact described in Section 3.6 of this NSA shall have sufficient authority over any of the Applicant-Parties' employees who may handle Classified 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 NSA; and

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

The Applicant Parties shall submit the Information Security Plan to the USG parties within ninety (90) days of this NSA's Effective Date.

3.8 **Nondisclosure of Protected Data**. The Applicant-Parties and their Affiliates shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, or Sensitive Information to any third party, or to any officer, director, shareholder, employee, agent, or contractor of the Applicant-Parties or their Affiliates, including those who serve in a supervisory, managerial or executive role with respect to the employees working with the information, unless disclosure has been approved by prior written consent obtained from DHS and DOJ, or there is an official need for disclosure of the information in order to fulfill an obligation consistent with the purpose for which the information is collected or maintained.

3.9 **Notice of Obligations**. The Applicant-Parties shall instruct appropriate officials, employees, contractors, and agents as to the Applicant-Parties' obligations under this NSA, including the individuals' duty to report any violation of this NSA and the reporting requirements in Article 4 of this NSA, and shall issue periodic reminders to them of such obligations. The Applicant-Parties shall have issued these instructions in writing within forty-five (45) days of the Effective Date, and shall submit them to the U.S. Government parties at the same time as it issues the instructions to officials, employees, contractors and agents.

3.10 **Access to Classified or Sensitive Information**. Nothing contained in this NSA shall limit or affect the authority of a U.S. Government Authority to deny, limit or revoke whatever access the Applicant-Parties or their Affiliates might have to Classified or Sensitive Information under that Government Authority's jurisdiction.

ARTICLE 4: DISPUTES

4.1 **Informal Resolution**. The Parties shall use their best efforts to resolve any disagreements that may arise under this NSA. Disagreements shall be addressed, in the first instance, at the staff level by the Parties' designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to the legal counsel for the Applicant-Parties, the Assistant Attorney General for the National Security Division of DOJ, and the Assistant Secretary for Policy of DHS, or their respective designees, unless DHS or DOJ believes that important national interests can be protected, or the Applicant-Parties believe that paramount commercial interests can be resolved, only be resorting to the measures set forth in Section 6.2. If, after meeting with higher authorized officials, any of the Parties determines that further negotiation would be fruitless, then that Party may resort to the remedies set forth in Section 6.2. If resolution of a disagreement requires access to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances for the purpose of resolving that disagreement.

4.2 **Enforcement of Agreement**. Subject to Section 6.1 of this NSA, if any of the Parties believes that any other party has breached or is about to breach this NSA, that Party may bring an action against the other Party for appropriate judicial relief. Nothing in this NSA shall limit or affect the right of a U.S. Government Agency to:

(a) require that the Party or Parties believed to have breached, or about to breach, this NSA cure such breach within thirty (30) days, or whatever shorter time period is appropriate under the circumstances, upon receiving written notice of such breach;

(b) request that the FCC modify, condition, revoke, cancel or render null and void any license, permit, or other authorization granted or given by the FCC to any of the Applicant-Parties or their Affiliates, request that the FCC take other action, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against the Applicant-Parties or their Affiliates;

(c) seek civil sanctions for any violation by the Applicant-Parties or their Affiliates of any U.S. law or regulation or term of this NSA;

(d) pursue criminal sanctions against the Applicant-Parties or their Affiliate, or any director, officer, employee, representative, or agent of the Applicant-Parties or their Affiliates, or against any other person or entity, for violations of the criminal laws of the United States; or

(e) seek suspension or debarment of the Applicant-Parties or their Affiliates from eligibility for contracting with the U.S. Government.

4.3 **Irreparable Injury**. The Applicant-Parties agree that the United States would suffer irreparable injury if for any reason the Applicant-Parties failed to perform any of their obligations under this NSA, and that monetary relief would not be an adequate remedy.

Accordingly, the Applicant-Parties agree that, in seeking to enforce this NSA, DHS and DOJ shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

4.4 **Waiver**. The availability of any civil remedy under this NSA shall not prejudice the exercise of any other civil remedy under this NSA 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 NSA, 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

4.5 **Waiver of Immunity**. The Applicant-Parties agree that, to the extent that it or any of its property (including FCC licenses and authorizations and intangible property) is or becomes entitled at any time to any immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of Government from any legal action, suit or proceeding or from setoff or counterclaim relating to this NSA, from the jurisdiction of any competent court or the FCC, from service of process, from attachment prior to judgment, from attachment in aid of execution of a judgment, from execution pursuant to a judgment or arbitral award, or from any other legal process in any jurisdiction, it, for itself and its property expressly, irrevocably and unconditionally waives, and agrees not to plead or claim, any such immunity with respect to matters arising with respect to this NSA or the obligations herein (including any obligation for the payment of money) in any proceeding brought by a U.S. federal, state, or local Government Authority. The Applicant-Parties agree that the waiver in this provision is irrevocable and is not subject to withdrawal in any jurisdiction or under any statute, including the Foreign Sovereign Immunity Act, 28 U.S.C. § 1602 et seq. The foregoing waiver shall constitute a present waiver of immunity at any time any action is initiated by a U.S. federal, state, or local Government Authority against the Applicant-Parties or their Affiliates with respect to compliance with this NSA.

4.6 **Forum Selection**. It is agreed by and between the Parties that a civil action among the Parties for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this NSA shall be brought, if at all, in the United States District Court for the District of Columbia.

ARTICLE 5: REPORTING AND NOTICE

5.1 **Filings Concerning *de jure* or *de facto* Control of any of the Applicant-Parties**. If any of the Applicant-Parties or their Affiliates makes any filing with the FCC or any other Government Authority relating to the *de facto* or *de jure* control of any of the Applicant-Parties or their Affiliates, or any Cable System, except for filings with the FCC for assignments or

transfers of control that are pro forma, the Applicant-Parties shall promptly provide to DHS and DOJ written notice and copies of such filing.

5.2 **Change in Control**. If any member of the management of the Applicant-Parties or their Affiliates (including officers and members of the Board of Directors) acquires any information that reasonably indicates that any single foreign entity or individual has or will likely obtain an ownership interest (direct or indirect) in any of the Applicant-Parties or their Affiliates, or in any Cable System, above ten (10) percent, as determined in accordance with 47 C.F.R. § 63.09, or if any foreign entity or individual, singly or in combination with other foreign entities or individuals, has or will likely otherwise gain either: (i) Control; or (ii) *de facto* or *de jure* control of any of the Applicant-Parties or their Affiliates then such officer or director shall promptly cause the Applicant-Parties to notify DHS and DOJ in writing within ten (10) business days. Notice under this Section shall, at a minimum:

(a) identify the entity or individual(s) (specifying the name, addresses, and telephone numbers of the entity);

(b) identify the beneficial owners of the increased or prospective increased interest in the Applicant-Party or Affiliate by the entity or individual(s) (specifying the name, addresses, and telephone numbers of each beneficial owner); and

(c) quantify the amount of ownership interest that the entity or individual(s) has or will likely obtain in the Applicant-Party or Affiliate and, if applicable, the basis for their prospective Control of the Applicant-Party or Affiliate.

5.3 Procedure and Process on Reporting. Within forty-five (45) days of the Effective Date, the Applicant-Parties and their Affiliates shall adopt and distribute to all officers and directors, a written procedure or process for the reporting by officers and directors of noncompliance with this NSA. This written procedure or process shall also provide for the reporting by employees, agents and contractors to management of information that must be reported to DHS or DOJ under this Article. Any violation by any of the Applicant-Parties or their Affiliates of any material term of such corporate policy shall constitute a breach of this NSA. By a written statement, the Applicant-Parties and their Affiliates shall notify all employees, contractors and agents that the general categories of information identified in this Article should be disclosed to senior management and shall set forth in a clear and prominent manner the contact information for a senior manager to whom such information may be reported. The written statement informing employees, contractors, and agents of the need to report this information shall also state that the Applicant-Parties and their Affiliates will not discriminate against, or otherwise take adverse action against, anyone who reports such information to management or the United States government. The company may make such process or procedure documents available to one or more U.S. Government Party upon the U.S. Government Party's (Parties') request.

5.4 **Non-retaliation**. Within forty-five (45) days after the Effective Date, the Applicant-Parties and their Affiliates shall, by duly authorized action by its Board of Directors, adopt and distribute to all officers and directors an official corporate policy that strictly prohibits the Applicant-Parties or their Affiliates from discriminating or taking any adverse action against any officer, director, employee, contractor, or agent because he or she has in good faith initiated or attempted to initiate a notice or report under this Article, or has notified or attempted to notify the management to report information that he or she believes in good faith is required to be reported to DHS and DOJ under either this Article or under the Applicant-Parties' or their Affiliates' written notices to employees on the reporting of any such information. Any violation by any of the Applicant-Parties or their Affiliates of any material term of such corporate policy shall constitute a breach of this NSA. The company may make such process or procedure documents available to one or more U.S. Government party upon the U.S. Government party's (parties') request.

5.5 **Reporting of Incidents**. The Applicant-Parties shall report to DHS and DOJ any information acquired by the Applicant-Parties or any of its officers, directors, employees, contractors or agents that reasonably indicates:

(a) a breach of this NSA;

(b) access to or disclosure of Domestic Communications, or the conduct of Electronic Surveillance, in violation of federal, state or local law or regulation;

(c) access to or disclosure of CPNI or Subscriber Information in violation of federal, state or local law or regulation (except for violations of FCC regulations relating to improper commercial use of CPNI); or

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

This report shall be made in writing by the appropriate Applicant-Party officer to DHS and DOJ, no later than ten (10) days after the Applicant-Party acquires information indicating a matter described in this Section. The Applicant-Parties and their Affiliate shall lawfully cooperate in investigating the matters described in this Section. The Applicant-Parties and their Affiliates need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

5.6 **Access to Information and Facilities**. DHS or DOJ may visit, at any time, any part of the Applicant-Parties' Domestic Communications Infrastructure and security offices to conduct on-site reviews concerning the implementation of the terms of this NSA and may at any time require unimpeded access to information concerning technical, physical, management, or other security measures needed by DHS or DOJ to verify compliance with the terms of this NSA.

5.7 **Access to Personnel**. Upon reasonable notice from DHS or DOJ, the Applicant-Parties shall make available for interview any officer or employee of the Applicant-Parties, and any contractor located in the United States, who is in a position to provide information to verify compliance with the terms of this NSA.

5.8 **Annual Report**. On or before the last day of January of each year, a designated senior corporate officer representing each of the Applicant-Parties shall submit to DHS and DOJ a report assessing the Applicant-Parties' compliance with the terms of this NSA for the preceding calendar year. The report shall include:

(a) a copy of the then current policies and procedures adopted to comply with this NSA;

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

(c) an updated list of Principal Equipment, as defined in Section 2.6, including but not limited to any material changes or upgrades to system components or applications since the list was most recently provided to the USG Parties; and

(e) identification of any other issues that, to the Applicant-Parties' knowledge, will or reasonably could affect the effectiveness of or its compliance with this NSA.

5.9 **Notices**. Effective upon execution of this NSA by all the Parties, all notices and other communications relating to this NSA, such as a proposed modification, shall be in writing and shall be deemed given as of the date of receipt and shall be sent by electronic mail (if an email is specified below or in a subsequent notice) and one of the following methods: (a) delivered personally, (b) sent by facsimile, (c) sent by documented overnight courier service, or (d) sent by registered or certified mail, postage prepaid, addressed to the Parties' designated representatives at such addresses as the parties may designate in accordance with this Section:

Department of Justice
Assistant Attorney General
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530
ttelecom@usdoj.gov

Department of Homeland Security
Assistant Secretary
Office of Policy
C/O Director, Foreign Investment Risk Management
245 Murray Lane, SW
Mail Stop: 0445

Washington, D.C. 20528
ip-fcc@hq.dhs.gov

Denis Lesueur, President and CEO
Auto-Guadeloupe Investissement S.A.
Global Caribbean Fiber SAS
Global Caribbean Network SAS
Tour Secid, 8th Floor
Place de la Renovation, 97110
Point-a-Pitre, Guadeloupe
France
Denis.lesueur@loret.net

Eric Fishman, Counsel for AGI, GCN and GCF
Fishman Advisors PLLC
400 Central Park West
Apt. 3R
New York, New York 10025
eric@fishmanadvisors.com

ARTICLE 6: FCC CONDITION

6.1 **FCC Approval**. Upon the execution of this NSA by all the Parties, DHS and DOJ and the Applicant-Parties shall jointly request that the FCC adopt a condition substantially the same as set forth in Exhibit A attached hereto (the "Condition to FCC Authorization") applicable to the submarine cable landing license granted to GCN on September 13, 2005 (xxx).

6.2 **Right to Object to Future FCC Filings**. The Applicant-Parties agree that in any application or petition by any of the Applicant-Parties or their Affiliates to the FCC for licensing or other authority filed with or granted by the FCC after the execution of this NSA, except with respect to *pro forma* assignments or *pro forma* transfers of control, the Applicant-Party shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this NSA. Notwithstanding Section 7.9, DHS and DOJ reserve the right to object, formally or informally, to the grant of any other FCC application or petition of any of the Applicant-Parties or their Affiliates for a license or other authorization under Titles II and III of the Communications Act of 1934, as amended, and to seek additional or different terms that would, consistent with the public interest, address any threat to the ability of the United States to enforce the laws, preserve the national security, and protect the public safety raised by the services and transactions underlying ay such application or petition.

ARTICLE 7: OTHER

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

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

7.3 **Other Laws**. Nothing in this NSA is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local laws on the Applicant-Parties or their Affiliates, (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority the U.S. Government may possess over the activities or facilities of the Applicant-Parties or their Affiliates located within or outside the United States (including authority pursuant to the International Emergency Economic Powers Act). Nothing in this NSA is intended to or is to be interpreted to require the Parties to violate any applicable U.S. law.

7.4 **Statutory References**. All references in this NSA to statutory provisions shall include any future amendments to such statutory provisions.

7.5 **Non-Parties**. Nothing in this NSA is intended to confer or does confer any rights on any person other than the parties and the Government Authorities that utilize Lawful U.S. Process.

7.6 **Entire Agreement; Modifications**. This NSA constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, of the Parties with respect to the subject matter. This NSA may only be modified by written agreement signed by all of the Parties. DHS and DOJ agree to consider promptly and in good faith possible modifications to this NSA if the Applicant-Parties believe that the obligations imposed on it under this NSA 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, and public safety concerns. Any substantial modification to this NSA shall be reported to the FCC within thirty (30) days after approval in writing by the Parties.

7.7 **Severability**. The provisions of this NSA shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this NSA or the application of any provision thereof.

7.8 **Changes in Circumstances for the Applicant-Parties**. DHS and DOJ agree to negotiate in good faith and promptly with respect to at request by the Applicant-Parties for relief from application of specific provisions of this NSA if there is a change in circumstances such that those provisions become unduly burdensome or have a demonstrably adverse effect on the Applicant-Parties' or their Affiliates' competitive position.

7.9 **Changes in Circumstances for DHS or DOJ**. If after the date that all the Parties have executed this NSA, DHS or DOJ finds that the terms of this NSA are inadequate to address national security, law enforcement, or public safety concerns, then the Applicant-Parties will negotiate in good faith to modify this NSA to address those concerns.

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

7.11 **Successors and Assigns**. This NSA shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns. This NSA shall also be binding on all subsidiaries, divisions, departments, branches, and other components or agents of the Applicant-Parties and their Affiliates.

7.12 **Effectiveness of Agreement**. Except as otherwise specifically provided in the provisions of this NSA, the obligations imposed and rights conferred by this NSA shall take effect upon the Effective Date.

7.13 **Notice of Additional Services**. The Applicant-Parties shall provide a minimum of thirty (30) days advanced notice to DHS and DOJ in the event that any Applicant-Party or Affiliate changes or intends to change the technical or operational plans set forth in the Recitals to this NSA such that the material representations made therein are no longer fully accurate, true and complete.

[Signature Pages Follow]

This NSA is executed on behalf of the Parties:

Auto-Guadeloupe Investissement, S.A.
Global Caribbean Fiber SAS
Global Caribbean Network SAS

Date: September 2, 2014

By: _____
Printed Name: Denis Lesueur
Title: President and CEO

Department of Homeland Security

Date: _____

By: _____
Printed Name: Alan Bersin
Title: Assistant Secretary

United States Department of Justice

Date: _____

By: _____
Printed Name: John Carlin
Title: Assistant Attorney General

EXHIBIT A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses granted thereunder are subject to the compliance of Auto-Guadeloupe Investissement S.A. ("AGI"), Global Caribbean Fiber S.A. ("GCF") and Global Caribbean Network SAS ("GCN") with the provisions of the agreement (the "Agreement") between AGI, GCF, and GCN, on the one hand, and the Department of Homeland Security ("DHS"), and the Department of Justice ("DOJ"), on the other, dated August __, 2014, as executed by AGI, GCF and GCN, which Agreement is designed to address national security, law enforcement, and public safety concerns of DHS and DOJ regarding the authority granted herein. Nothing in the Agreement, as amended, is intended to limit any obligation imposed by federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(l) and the FCC's implementing regulations.

This NSA is executed on behalf of the Parties:

Auto-Guadeloupe Investissement, S.A.
Global Caribbean Fiber SAS
Global Caribbean Network SAS

Date: September 2, 2014

By: _____
Printed Name: Denis Lesueur
Title: President and CEO

Department of Homeland Security

Date: 9/5/2014

By: _____
Printed Name: Alan Bersin
Title: Assistant Secretary

United States Department of Justice

Date: _____

By: _____
Printed Name: John Carlin
Title: Assistant Attorney General

This NSA is executed on behalf of the Parties:

Auto-Guadeloupe Investissement, S.A.
Global Caribbean Fiber SAS
Global Caribbean Network SAS

Date: _____

By: _____
Printed Name: Denis Lesueur
Title: President and CEO

Department of Homeland Security

Date: _____

By: _____
Printed Name: Alan Bersin
Title: Assistant Secretary

United States Department of Justice

Date: 9/6/14

By: _____
Printed Name: Richard Sofield
Title: Director, Foreign Investment Review Staff, National Security Division