

AGREEMENT

THIS AGREEMENT (the “**Agreement**”) is made as of the date of the last signature affixed hereto, by and between American Samoa Hawaii Cable, LLC and AST Telecom, LLC (referred to collectively as the “**Applicants**”) on the one hand, and the U.S. Department of Homeland Security (“**DHS**”), on the other (each referred to individually as a “**Party**” and collectively as the “**Parties**”).

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 Homeland Security Presidential Directive / HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection);

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

WHEREAS, American Samoa Hawaii Cable, LLC, Pac-Rim Redeployment, LLC and AST Telecom, LLC, all companies organized under the laws of Delaware, have jointly applied¹ to the Federal Communications Commission (“FCC”) for a license to land and operate a private fiber-optic submarine cable network (the “American Samoa-Hawaii Cable System” or “ASHC System”) between United States and the Independent State of Samoa, with landing stations at Keawaula in Hawaii, Iliili in American Samoa, and Apia, Samoa;

WHEREAS, American Samoa Hawaii Cable, LLC will acquire all ownership rights in the ASHC System held by Pac-Rim Redeployment, LLC upon the commissioning of the ASHC System, including the wet-link and shore-end segments of the ASHC System;

WHEREAS, the Applicants will own and operate a landing station and Network Operations Center in Iliili, and will lease space at an existing landing station in Keawaula from AT&T, Inc., but will not own or control the foreign landing station in Apia;

WHEREAS, the ASHC System will provide telecommunications services to and from the United States which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, the Applicants will have direct physical and electronic access to a variety of

¹ Federal Communications Commission File No. SCL-LIC-20080814-00016, filed on August 13, 2008.

customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

WHEREAS, the Applicants have an obligation to protect from unauthorized disclosure the contents of wire and electronic communications to and from the United States under U.S. law;

WHEREAS, DHS will request that the FCC's grant of the Applicants' pending submarine cable landing license application be made subject to resolution of issues relating to national security, law enforcement, and public safety, and whereas the Applicants have agreed to enter into this Agreement with DHS to address issues raised by DHS and to jointly petition that the FCC condition the requested authorization on compliance with this Agreement;

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

1.1 **“Applicants”** means American Samoa Hawaii Cable, LLC and AST Telecom, LLC, and all Affiliates and all subsidiaries.

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 American Samoa Hawaii Cable, LLC or AST Telecom, LLC owns or Controls.

1.4 **“Cable System”** means all equipment, facilities and services pertaining to the ASHC System, and any other cable system owned or Controlled by the Applicants that lands in the United States; 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 1954, 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 Section 1.6(a) through (d); or
- (f) either of the Applicants' obligations under this Agreement.

1.7 “**CPNI**” means Consumer Proprietary Network Information.

1.8 “**De facto**” and “**de jure**” control have the meanings provided in 47 C.F.R. § 1.2110.

1.9 “**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.

1.10 “**Domestic Communications Infrastructure**” means any portion of the Cable System used by or on behalf of the Applicants 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 facilities controlled by entities with which the Applicants 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 Applicants that are:

- (1) interconnecting communications providers; or
- (2) providers of services or content that are:
 - (A) accessible using the communications services of the Applicants; and
 - (B) available in substantially similar form and on commercially reasonable terms through communications services of companies other than the Applicants.

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

1.12 “**Electronic Communication**” has the meaning given it in 18 U.S.C. § 2510(12).

1.13 “**Electronic Surveillance**,” for the purposes of this Agreement, 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.

1.14 “**Foreign**” where used in this Agreement, whether capitalized or lower case, means non-U.S.

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

1.16 “**Intercept**” or “**Intercepted**” has the meaning defined in 18 U.S.C. § 2510(4).

1.17 “**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.

1.18 “**Management of the Applicants**” means the companies’ officers and members of their Board of Directors.

1.19 “**Network Management Information**” means network management operations plans, processes and procedures; descriptions of the placement of NOC(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; network performance information; and network access ability and procedures..

1.20 “**Principal Equipment**” means the primary electronic components of a submarine cable system, to include the hardware used at the NOC(s), landing station(s) and the cable itself, such as servers, 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 synchronous optical network (SONET), synchronous digital hierarchy (SDH), wave division multiplexing (WDM), dense wave division multiplexing (DWDM), coarse wave division multiplexing (CWDM) or optical carrier network (OCx) equipment, as applicable.

1.21 “**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 63.24 of the FCC's Rules (47 C.F.R. § 63.24).

1.22 “**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 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; 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,” “Protected Critical Infrastructure Information,” or other similar designations.

1.23 “**Subscriber Information**” means all records or other information relating to customers or subscribers of the Applicants 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.

1.24 “**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, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, 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.

1.25 “**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.

1.26 “**Wire Communication**” has the meaning given it in 18 U.S.C. § 2510(1).

1.27 **Other Definitional Provisions.** Other capitalized terms used in this Agreement and 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 as well as to the feminine and neuter genders of such term. Whenever the words “include,” “includes,” or “including” are used in this Agreement, they shall be deemed to be followed by the words “without limitation.”

ARTICLE 2: OPERATIONS, FACILITIES, INFORMATION STORAGE AND ACCESS

2.1 **Operational Requirements.** With respect to the operation of the Cable System, the Applicants agree as follows:

- (a) the Applicants shall have the ability to promptly and effectively interrupt in whole or in part traffic to and from the United States on the Cable System by disabling or disconnecting circuits at the U.S. cable landing;
- (b) the Applicants shall have the ability to isolate the U.S. landing stations and the connecting cable segment from the rest of the Cable System and to restore and continue service on this segment, separate from the rest of the Cable System; and
- (c) the Cable System shall be configured so that the NOC will be able to view the status of the Cable System and individual cable segments.

2.2 **Compliance with Lawful U.S. Process.** The Applicants shall configure the Domestic Communications Infrastructure to be capable of complying, and the employees of the Applicants 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 the Cable Landing License Act of 1921, as amended (47 U.S.C. §§ 34-39)

and Executive Order 10530 § 5(a), reprinted as amended in 3 U.S.C. § 301, and § 706 of the Communications Act of 1934, as amended, (47 U.S.C. § 606); 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.*).

2.3 **Cable System Infrastructure.** Within **ten (10) business days** after the Effective Date the Applicants shall provide to DHS a finalized list of:

- (a) the Principal Equipment used in all the Cable System, to include information on the Principal Equipment's manufacturer and model; and
- (b) all contracts held by the Applicants for the maintenance and security of the Cable System.

The Applicants shall provide at least **fifteen (15) business days'** advance written notice to DHS prior to performing any maintenance, repair, or replacement that would result in any modification to the Principal Equipment list for the Cable System. The Applicants need not comply with the advance notice requirement for any maintenance, repair or replacement that is undertaken pursuant to a bona fide emergency and is necessary to ensure the continued operability of the Cable System; however, in such circumstances the Applicants shall provide advance notice of the modification to DHS if practicable, and if impracticable, within **fifteen (15) business days** after the modification of the Principal Equipment located at Keawaula and **(30) business days** after the modification for all other Principal Equipment. The Applicants shall provide at least **thirty (30) business days'** advance written notice to DHS prior to making any modifications to its list of contracts for Cable System maintenance and security. The Applicants agree to make the Network Management Information available to DHS upon request. The Applicants shall negotiate in good faith to resolve any national security, law enforcement or public safety concerns DHS may raise with respect to the Cable System's Principal Equipment, contracts, and Network Management Information.

2.4 **Information Storage and Access.** Unless otherwise agreed to by the Parties, the Applicants shall make the following available in the United States:

- (a) stored Domestic Communications, if such communications are stored by or on behalf of either of the Applicants 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 either of the Applicants, if such communications are stored by or on behalf of either of the Applicants for any reason;
- (c) Transactional Data, if such data are stored by or on behalf of either of the Applicants for any reason;
- (d) Subscriber Information, if such information is stored by or on behalf of either of the Applicants for any reason; and

- (e) billing records of customers or subscribers, if such information is stored by or on behalf of either of the Applicants for any reason.

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 either of the Applicants have contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

2.5 **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 either of the Applicants, including any information that is listed in Section 2.4 above, the Applicants shall ensure such preserved records or other evidence are stored in the United States.

2.6 **Compliance with U.S. Law**. Nothing in this Agreement shall excuse the Applicants 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.

2.7 **Storage of Protected Information**. The Applicants shall store all Classified Information and Sensitive Information exclusively in the United States.

ARTICLE 3: SECURITY

3.1 **Measures to Prevent Improper Use or Access**. The Applicants shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to 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 Agreement. The Applicants shall submit the policies and procedures regarding these measures to DHS for review upon request. The Applicants agree to meet and confer with DHS and reasonably address any concerns DHS may raise about the policies or the procedures described therein.

3.2 **Access by Foreign Government Authorities**. The Applicants 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 either of the Applicants 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 or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process shall be reported to DHS 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 either of the Applicants. The Applicants shall take reasonable measures to ensure that they each will promptly learn of all such requests or submission of legal process. Provided, however, that nothing in this Section 3.2 shall require the express written consent of DHS or the authorization of a court of competent jurisdiction in the

United States with respect to any response to the legal process, or the request of or on behalf of the Independent State of Samoa, identified representative, component or subdivision thereof with respect to the non-U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that may originate or terminate outside the United States.”

3.3 **Disclosure to Foreign Government Authorities.** The Applicants 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 or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a Foreign Government, an identified representative, a component or subdivision thereof to either of the Applicants for the communications, data or information identified that is maintained by either of the Applicants shall be referred to DHS 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 either of the Applicants, unless the disclosure of the request or legal process would violate applicable law. The Applicants shall take reasonable measures to ensure that they will promptly learn of all such requests or submission 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 Applicants shall notify DHS 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 Applicants shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified and Sensitive Information in accordance with U.S. federal and state law or regulation and this Agreement.

3.6 **Point of Contact.** The Applicants have heretofore designated a Point of Contact 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 Applicants agree that the designated Point of Contact, or an alternate Point or Points of Contact, shall be responsible for receiving and addressing any national security, law enforcement or public safety concerns raised by DHS regarding the Cable System, and shall have the authority to negotiate measures to mitigate such concerns. The Applicants shall ensure that at least one such Representative 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 responding to inquiries from DHS concerning the Applicants' compliance with the terms of this Agreement, 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 to the customers or subscribers of the Applicants. If the designee cannot satisfy these requirements, the Applicants shall in **ten (10) business days** or less notify DHS in writing of a new Point or Points of Contact. The Applicants shall notify DHS of all other future changes in such designation, or the designation of alternate Points of Contact, also in **ten (10) business days** or fewer. The Point(s) of Contact shall be a resident U.S. national or nationals who, based on the information in the Applicants' possession, are eligible for appropriate U.S. security clearances. The Applicants shall cooperate with any request by a Government Authority within the United States that a background check, security clearance process or both be completed for a Point of Contact.

3.7 **Information Security Plan.** Within **ninety (90) calendar days** of the Effective Date the Applicants shall:

- (a) take appropriate measures to prevent unauthorized Access to data or facilities that might contain Classified or Sensitive Information;
- (b) assign U.S. nationals, 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 provide the name, date of birth, and other relevant requested 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 to Executive Order 12968;
- (e) provide that the Point(s) of Contact described in Section 3.6 of this Agreement shall have sufficient authority over any employees or contractors of the Applicants 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 Agreement; and
- (f) maintain appropriately secure facilities (e.g., offices) for the handling and storage of any Classified or Sensitive Information.

The Applicants shall make the policies and procedures regarding their respective Information Security Plans available to DHS upon request.

3.8 **Nondisclosure of Protected Data.** The Applicants 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 Applicants, 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 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 Applicants shall instruct appropriate officials, employees, contractors, and agents as to their obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in Article 4 of this Agreement, and shall issue periodic reminders to them of such obligations.

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

ARTICLE 4: REPORTING AND NOTICE

4.1 **Filings Concerning *de jure* or *de facto* Control of the Applicants.** If either of the Applicants makes any filing with the FCC or any other Government Authority relating to the *de facto* or *de jure* control of that Applicant, or to the Cable System, except for filings with the FCC for assignments or transfers of control that are *pro forma*, the Applicants shall promptly provide to DHS written notice and copies of such filing.

4.2 **Change in Control.** If any member of the managements of the Applicants (including officers and members of the Boards of Directors) acquires any information that reasonably indicates that any single foreign entity or individual, other than those already identified in connection with the pending FCC Application filed by the Applicants, has or will likely obtain an ownership interest (direct or indirect) in either of the Applicants, or in the 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 either of the Applicants then such officer or director shall promptly cause that Applicant to notify DHS 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 or the Cable System 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 or the Cable System and, if applicable, the basis for their prospective Control of the Applicant or the Cable System.

4.3 **Procedure and Process on Reporting.** Within **forty-five (45) calendar days** of the Effective Date, the Applicants 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 Agreement. 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 under this Article. Any violation by either of the Applicants of any material term of such corporate policy shall constitute a breach of this Agreement. By a written statement, the Applicants 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 Applicants will not discriminate against, or otherwise take adverse action against, anyone who reports such information to management or the United States government. The Applicants shall make such process or procedure documents available to DHS upon request.

4.4 **Non-retaliation.** Within **forty-five (45) calendar days** after the Effective Date, the Applicants shall adopt and distribute to all officers and directors an official corporate policy that strictly prohibits discrimination or 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 under either this Article or under the Applicants' written notices to employees on the reporting of any such information. Any violation by either of the Applicants or any of their Affiliates of any material term of such corporate policy shall constitute a breach of this Agreement. The Applicants shall make such process or procedure documents available to DHS upon request.

4.5 **Reporting of Incidents.** The Applicants shall report to DHS any information acquired by any of their officers, directors, employees, contractors or agents that reasonably indicates:

- (a) a breach of this Agreement;
- (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 officer to DHS no later than **ten (10) calendar days** after either of the Applicants acquires information indicating a matter described in this Section. The Applicants shall lawfully cooperate in investigating the matters described in this Section. The Applicants 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.

4.6 **Access to Information and Facilities.** DHS, or other agencies or personnel assigned to assist DHS, may visit at any time any part of the Applicants' Domestic Communications

Infrastructure and security offices to conduct on-site reviews concerning the implementation of the terms of this Agreement and may at any time require unimpeded access to information concerning technical, physical, management, or other security measures needed by DHS to verify compliance with the terms of this Agreement.

4.7 **Access to Personnel**. Upon reasonable notice from DHS, or other agencies or personnel assigned to assist DHS, the Applicants shall make available for interview any of their officers or employees and any contractor located in the United States, who is in a position to provide information to verify compliance with the terms of this Agreement.

4.8 **Annual Report**. On or before the last day of January of each year, designated senior corporate officers representing each of the Applicants shall submit to DHS a report assessing each of the Applicants' compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

- (a) a copy of the then current policies and procedures adopted to comply with this Agreement;
- (b) a summary of the changes, if any, to the policies or procedures, and the reasons for those changes;
- (c) a summary of any known acts of noncompliance with the terms of this Agreement, 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; and
- (d) identification of any other issues that, to either of the Applicants' knowledge, will or reasonably could affect the effectiveness of or its compliance with this Agreement.

4.9 **Notices**. Effective upon execution of this Agreement by the Parties, all notices and other communications relating to this Agreement, 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, or if no e-mail is specified, by 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 the addresses shown below, or to such other representatives at such addresses as the Parties may designate in accordance with this Section:

Department of Homeland Security
Assistant Secretary for Policy
Washington, DC 20528
ip-fcc@dhs.gov

American Samoa Hawaii Cable, LLC
P.O. Box 7870
Pago Pago, AS 96799
(684) 699-2100

AST Telecom, LLC
d/b/a Blue Sky Communications
Lafou Plaza
P.O. Box 478
Pago Pago, AS 96799
(684) 699-2759

With a copy to:

Kent Bressie
Harris, Wiltshire & Grannis LLP
1200 18th Street, N.W. Suite 1200
Washington, DC 20036-2516
202-730-1337 tel
202-730-1301 fax
kbressie@harriswiltshire.com

ARTICLE 5: FCC CONDITION

5.1 **FCC Approval**. Upon the execution of this Agreement by the Parties DHS shall on its own motion at an appropriate time or at the request of either of the Applicants notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Exhibit A attached hereto (the “Condition to FCC Authorization”), DHS has no objection to the FCC’s grant of the pending Application described in the Recitals of this Agreement. This Section is effective upon the Effective Date, provided however that in the case of a material modification or withdrawal of the Application after the execution of this Agreement the effectiveness of this Section may be suspended by DHS, and any such FCC filing is subject to the right to object reserved in Section 5.2.

5.2 **Right to Object to Future FCC Filings**. The Applicants agree that in any application or petition by either of the Applicants to the FCC for licensing or other authority related to any Cable System filed with or granted by the FCC after the execution of this Agreement, except with respect to *pro forma* assignments or *pro forma* transfers of control, the Applicant shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 7.9, DHS reserves the right to object, formally or informally, to the grant of any other FCC application or petition of either of the Applicants 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 any such application or petition.

ARTICLE 6:DISPUTES

6.1 **Informal Resolution**. The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. 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 Applicants and the Assistant Secretary for Policy of DHS, or their respective designees, unless DHS believes that important national interests can be protected, or the Applicants believe that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 6.2. If, after meeting with higher authorized officials, a Party 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.

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

- (a) require that the Party believed to have breached, or about to breach, this Agreement cure such breach within **thirty (30) calendar 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 the Applicants, 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 Applicants;
- (c) seek civil sanctions for any violation by either of the Applicants of any U.S. law or regulation or term of this Agreement;
- (d) pursue criminal sanctions against the Applicants, or any director, officer, employee, representative, or agent thereof, 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 Applicants from eligibility for contracting with the U.S. Government, in accordance with applicable law and regulation.

6.3 **Irreparable Injury**. The Applicants agrees that the United States would suffer irreparable injury if for any reason they failed to perform any of their obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, the Applicants agree that, in seeking to enforce this Agreement, DHS shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

6.4 **Waiver**. The availability of any civil remedy under this Agreement shall not prejudice the exercise of any other civil remedy under this Agreement 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 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.

6.5 **Waiver of Immunity.** The Applicants agree, to the extent that they or any of their 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 Agreement, 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, they, for themselves and their respective 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 Agreement 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 Applicants agrees 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 Immunities 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 either of the Applicants with respect to compliance with this Agreement.

6.6 **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 Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

ARTICLE 7: OTHER

7.1 **Right to Make and Perform Agreement.** Each Party represents that it has and shall continue to have throughout the term of this Agreement the full right to enter into this Agreement and perform its obligations hereunder and that this Agreement is a legal, valid, and binding obligation of each Party enforceable in accordance with its terms.

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

7.3 **Other Laws.** Nothing in this Agreement is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local laws on the Applicants, (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 Applicants located within or outside the United States (including authority

pursuant to the International Emergency Economic Powers Act). Nothing in this Agreement 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 Agreement to statutory provisions shall include any future amendments to such statutory provisions.

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

7.6 **Entire Agreement; Modifications.** This Agreement 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 Agreement may only be modified by written agreement signed by all Parties. DHS agrees to consider promptly and in good faith possible modifications to this Agreement if either of the Applicants believes that the obligations imposed on it under this Agreement 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 Agreement shall be reported to the FCC within **thirty (30) calendar days** after approval in writing by the Parties.

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

7.8 **Changes in Circumstances for the Applicants.** DHS agrees to negotiate in good faith and promptly with respect to any request by the Applicants for relief from application of specific provisions of this Agreement if there is a change in circumstances such that those provisions become unduly burdensome or have a demonstrably adverse effect on the Applicants' competitive position.

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

7.10 **Counterparts.** This Agreement 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 Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns. This Agreement shall also be binding on all subsidiaries, divisions, departments, branches, and other components or agents of the Applicants.

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

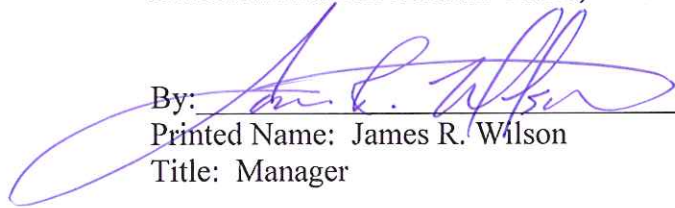
7.13 **Notice of Additional Services.** The Applicants shall provide a minimum of **thirty (30) calendar days** advanced notice to DHS in the event that they change or intend to change the technical or operational plans set forth in the Recitals to this Agreement such that the material representations made therein are no longer fully accurate, true and complete.

[Signature Pages Follow]

This Agreement is executed on behalf of the Parties:

American Samoa Hawaii Cable, LLC

Date: 1/5/09

By: 
Printed Name: James R. Wilson
Title: Manager

Date: _____

By: _____
Printed Name: Harley "Mike" Rollins
Title: Manager

AST Telecom, LLC

Date: _____

By: _____
Printed Name: Adolfo Montenegro
Title: President and CEO

Department of Homeland Security

Date: _____

By: _____
Printed Name: Stewart A. Baker
Title: Assistant Secretary for Policy

This Agreement is executed on behalf of the Parties:

American Samoa Hawaii Cable, LLC

Date: _____

By: _____

Printed Name: James R. Wilson

Title: Manager

Date: _____

By: Harley Z. Rollins

Printed Name: Harley "Mike" Rollins

Title: Manager

AST Telecom, LLC

Date: _____

By: _____

Printed Name: Adolfo Montenegro

Title: President and CEO

Department of Homeland Security

Date: _____

By: _____

Printed Name: Stewart A. Baker

Title: Assistant Secretary for Policy

American Samoa Hawaii Cable, LLC

Date: _____

By: _____
Printed Name: James R. Wilson
Title: Manager

Date: _____

By: _____
Printed Name: Harley "Mike" Rollins
Title: Manager

AST Telecom, LLC

Date: 12/30/2008

By: 
Printed Name: Adolfo Montenegro
Title: President and CEO

Department of Homeland Security

Date: _____

By: _____
Printed Name: Stewart A. Baker
Title: Assistant Secretary for Policy

This Agreement is executed on behalf of the Parties:

American Samoa Hawaii Cable, LLC

Date: _____

By: _____
Printed Name: James R. Wilson
Title: Manager

Date: _____

By: _____
Printed Name: Harley "Mike" Rollins
Title: Manager

AST Telecom, LLC

Date: _____

By: _____
Printed Name: Adolfo Montenegro
Title: President and CEO

Department of Homeland Security

Date: JANUARY 9, 2009


By: 
Printed Name: Stewart A. Baker
Title: Assistant Secretary for Policy

EXHIBIT A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses granted thereunder are subject to compliance with the provisions of the agreement (the “Agreement”) between **American Samoa Hawaii Cable, LLC** and **AST Telecom, LLC**, on the one hand, and the Department of Homeland Security (“**DHS**”), on the other, dated January 9, 2009, which Agreement is designed to address national security, law enforcement, and public safety concerns of DHS regarding the authority granted herein. Nothing in the Agreement 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)(1) and the FCC’s implementing regulations.