SECURITY AGREEMENT

This SECURITY AGREEMENT ("Agreement") is made as of the Effective Date by and between AP TeleGuam Holdings, Inc. ("AP TG"),[1] on behalf of itself and AP TeleGuam Merger Sub, LLC ("AP TeleGuam Merger Sub"), its wholly owned subsidiary created for purposes of the transaction subject to this Agreement through which AP TG will acquire TeleGuam Holdings, LLC ("TeleGuam Holdings"), GTA Telecom, LLC ("GTA Telecom"), GTA Services, LLC ("GTA Services"), and Pulse Mobile, LLC ("Pulse Mobile") (GTA TeleGuam, GTA Services, and Pulse Mobile, collectively, the "TeleGuam Licensees" and, together with TeleGuam Holdings, the "TeleGuam Entities," doing business as "GTA TeleGuam"), on the one hand, and the U.S. Department of Justice ("DOJ"), the U.S. Department of Homeland Security ("DHS"), and the U.S. Department of Defense ("DoD") on the other hand (collectively, "the USG Parties"), referred to individually by name or as "a Party" and collectively as "the Parties." Pursuant to the terms of the transaction subject to this Agreement, AP TeleGuam Merger Sub will merge with and into TeleGuam Holdings with TeleGuam Holdings continuing as the surviving entity. As a result of the merger, AP TG will become the new parent company of TeleGuam Holdings and thus the indirect parent of the TeleGuam Licensees.

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;

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

WHEREAS, all communications service providers have obligations to protect from unauthorized disclosure the contents of wire and electronic communications;

WHEREAS, the TeleGuam Licensees include GTA Telecom, holder of licenses supporting Guam's incumbent local exchange carrier (ILEC) managed by GTA TeleGuam;

---

[1] At the time of the proposed closing, AP TG will be jointly owned by three private investment funds that will collectively own approximately 97.2 percent of the company: (1) Advantage Partners IV, ILP (an Investment Limited Partnership with Japan citizenship, 42.2 percent), (2) AP Cayman Partners II, L.P. (Cayman Islands citizenship, 29.4 percent), and (3) Japan Ireland Investment Partners (Ireland citizenship, 25.6 percent).

GTA Services, also managed by GTA TeleGuam; as well as Pulse Mobile, LLC, a holder of licenses for common carrier cellular, Personal Communications Services (PCS) Broadband and Advanced Wireless Services (AWS), managed by GTA TeleGuam;

WHEREAS, TeleGuam Entities provide telecommunication services (also referred to as information and communications technology, or ICT) to federal government agencies and other commercial providers that supply ICT services to federal government agencies; in addition, certain service sharing arrangements exist between certain TeleGuam Entities and the U.S. Navy, a military service in the Department of Defense;

WHEREAS, according to the filings by AP TG and Shamrock TeleGuam Holdings, LLC (on behalf of the TeleGuam Entities) with the FCC,[2] the consummation of the proposed transaction will lead to a transfer of ownership and management of the TeleGuam Entities to APTG, with indirect ownership in the investment firms (1) Advantage Partners IV, ILP, (2) AP Cayman Partners II, L.P. and (3) Japan Ireland Investment Partners;

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

1.1. "Access" or "Accessible" means the ability to physically or logically undertake any of the following actions: (i) read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system or a network; (ii) add, edit or alter information or technology stored on or by software, hardware, a system or a network; and (iii) 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).

1.2. "Call Associated Data" means any information related to a Domestic Communication or related to the sender or recipient of Domestic Communication, to the extent the Domestic Communications Companies maintain such information in the normal course of business. Call Associated Data includes 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

[2] *See Joint Application of Shamrock TeleGuam Holdings, LLC, Transferor, GTA Telecom, LLC, GTA Services, LLC, Pulse Mobile, LLC, Licensees, and AP TeleGuam Holdings, Inc., Transferee, For Grant of Authority Pursuant to Section 214 of the Communications Act of 1934, as amended, and Sections 63.04 and 63.24 of the Commission's Rules to Complete a Transfer of Indirect Majority Ownership of the Licensees to AP TeleGuam Holdings, Inc.*, FCC, WC Docket No. 10-260 (filed Dec. 17, 2010), IBFS File Nos. ITC-T/C-20101216-00486 and ITC-T/C-20101216-00478 (filed Dec. 16, 2010); *Shamrock TeleGuam Holdings, LLC, Transferor, GTA Telecom, LLC, GTA Services, LLC, Pulse Mobile, LLC, Licensees, and AP TeleGuam Holdings, Inc., Transferee, Petition for Declaratory Ruling Under Section 310(b)(4) of the Communications Act, as Amended*, FCC, IBFS File No. ISP-PDR-20101216-00021 (filed Dec. 16, 2010); FCC, WT ULS File No. 0004531711 (filed Dec. 16, 2010).

number; conference-party numbers; post-cut through dial-digit extraction; in-band and out-of-band signaling; and party add, drop and hold.

1.3. "Classified Information" means information or technology that is classified according to Executive Order 13526 or any predecessor or successor executive order, or the Atomic Energy Act of 1954 or any statute that succeeds or amends the Atomic Energy Act of 1954.

1.4. "Control" and "Controls" means the power, direct or indirect, whether exercised, exercisable or not exercised, through any means employable, to decide, direct or otherwise influence matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause major business decisions to include:

(i) 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;

(ii) the dissolution of the entity;

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

(iv) the termination or non-fulfillment of contracts of the entity;

(v) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in subsections (i) through (iv) above; and

(vi) the Domestic Communications Companies' obligations under this Agreement.

1.5. "Customer Proprietary Network Information (CPNI)" means (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information, as that term is defined at 47 U.S.C. § 222.CPNI is understood to include Subscriber Information and Identifying Information as referred to herein.

1.6. "Data Centers" means (a) equipment (including firmware, software, hardware and upgrades), facilities, and premises used by (or on behalf of) one or more Domestic Communications Companies in connection with Hosting Services (including data storage and provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services), and (b) equipment hosted by the Domestic Communications Companies that is leased or owned by a Hosting Services customer.

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

1.8. "Domestic Communications" means (i) Wire Communications or Electronic

Communications (whether stored or not) from one U.S. location to another U.S. location and (ii) 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 (i) transmission, switching, bridging and routing equipment (including firmware, software, hardware, and upgrades) in use to provide, process, direct, control, supervise or manage Domestic Communications; and (ii) facilities and equipment that are used to control the equipment described in (i). Domestic Communications Infrastructure does not include equipment dedicated to the termination of international undersea cables, provided that such equipment is utilized solely to effectuate the operation of undersea transport network(s) outside of the United States and in no manner controls land-based transport network(s) or their associated systems in the United States, nor does it include facilities and equipment intended and capable solely of performing billing, customer management, business management or marketing functions.

1.10. "Domestic Communications Companies" means the TeleGuam Entities and all existing and post-Agreement subsidiaries, divisions, affiliates, departments, branches and other components of TeleGuam Holdings, or any other entity over which TeleGuam Holdings has *de facto* or *de jure* control, that (i) provide Domestic Communications, or (ii) engage in provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services, or data storage in connection with Hosting Services.

1.11. "Effective Date" means the date of the last signature affixed to this Agreement by the Parties.

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

1.13. "Electronic Surveillance" means:

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

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

(iii) acquisition of dialing, routing, addressing or signaling information through pen register or trap and trace devices or other devices or 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.;

(iv) acquisition of location- related information concerning a service subscriber or facility;

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

(vi) access to, or acquisition or interception of, or preservation of communications or information as described in (i) through (ii) above and comparable State laws.

1.14. "Foreign Entity" means any Foreign Person; any entity established under the laws of a country other than the United States, or any government other than the U.S. Government or a U.S. state or local government.

1.15. "Foreign Person" means any Person who is not a U.S. Person as provided by 31 C.F.R. § 800.222.

1.16. "Hosting Services" means Web hosting (whether shared or dedicated, and including design, server management, maintenance and telecommunications services), Web site traffic management, electronic commerce, streamed media services, server collocation and management, application hosting, and all other similar services offered by the Domestic Communications Companies.

1.17. "Identifying Information" means the name, address, telephone number, e-mail address, IP address, or any other information that is customarily used to identify a particular end user. Identifying Information is understood to be included within, and a subset of, CPNI.

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

1.19. "Interconnection Agreement" means an agreement pursuant to Section 251(c) of the Communications Act of 1934, as amended, 47 U.S.C. § 251(c), between the Domestic Communications Companies and a third-party telecommunications carrier that provides for interconnection, collocation, resale, network elements, and ancillary services between the parties.

1.20. "Lawful U.S. Process" means lawful U.S. federal, state, or local court orders, subpoenas, warrants, processes, or authorizations issued under U.S. federal, state, or local law for electronic surveillance, physical search or seizure, production of tangible things, or access to or disclosure of Domestic Communications, Call Associated Data, or U.S. Hosting Data, including Transactional Data, CPNI, or Subscriber Information.

1.21. "Merger Agreement" means the Agreement and Plan of Merger by and among APTG, AP TeleGuam Merger Sub, TeleGuam Holdings, Shamrock TeleGuam Holdings, LLC and STG Representative Holdings, LLC, as representative of the Members and Optionholders of TeleGuam Holdings, LLC (dated November 13, 2010).

1.22. "Network Management Information" means: network plans, processes and procedures; placement of Network Operations Center(s) and interfaces to other domestic and international carriers, ISPs or other critical infrastructures; descriptions of any networks and operations processes and procedures related to backbone infrastructure(s); description of any proprietary control mechanisms and operating and administrative software; and all network performance information.

1.23. "Network Operations Center" or "NOC" means: the locations, facilities, systems, and applications designated as such for purposes of performing network management, monitoring, and analysis, provisioning, fault management, security management, asset

management, maintenance or other functions for the Domestic Communications Companies' data, voice, radio, and transport networks.

1.24. "Party" and "Parties" have the meanings given them in the Preamble.

1.25. "Personnel" means an entity's (i) employees, officers, directors, and agents, and (ii) contract or temporary employees (part-time or full-time) who are under the direction and control of the entity and have Access to its products or services.

1.26. "Routine Business Visits" has the meaning given it in Section 3.4 of this Agreement.

1.27. Security Incident: A violation or imminent threat of violation of security policies, acceptable use policies, standard security practices, or Domestic Communications Companies' security policies (e.g., the Information Security policy) including, but not limited to: (i) attempts (either failed or successful) to gain unauthorized Access to a facility, system, computer network or data; (ii) unauthorized or unwanted disruption or denial of service; (iii) unauthorized Access or use of a system, network or computer resources for the processing or storage of data; (iv) unauthorized changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent; (v) unauthorized addition, alteration, deletion, acquisition, theft, transfer, diversion of or Access to Classified Information, Sensitive Information, Customer Proprietary Network Information, or Subscriber Information.

1.28. "Sensitive Information" means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Electronic Surveillance pursuant to Lawful U.S. Process, (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, and any other U.S. Government information that is designated in writing by an authorized official as "Sensitive Information," "For Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," "Not For Distribution to Foreign Nationals," "NOFORN," or other similar categories.

1.29. "Subscriber Information" means information relating to subscribers or customers of Domestic Communications Companies, including U.S. Hosting Services Customers (or the end-users of U.S. Hosting Services Customers), 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. Subscriber Information is understood to be included within, and a subset of, CPNI.

1.30. "Transaction" means the purchase of GTA TeleGuam by AP TG pursuant to the terms of the Merger Agreement.

1.31. "Transactional Data" means:

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

(ii) any information possessed by the Domestic Communications Companies relating to the identity or location of any customer, subscriber, account payer, or any end-user relating to all telephone numbers, domain names, IP addresses, Uniform Resource Locators ("URLs");

(iii) the time, date, size or volume of data transfers, duration, domain names, MAC or IP addresses (including source and destination), URLs, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics associated with any Domestic Communication, or other Wire or Electronic Communication within the definition of U.S. Hosting Data;

(iv) any information related to any mode of transmission (including mobile transmissions); and

(v) any information indicating the physical location to or from which a Domestic Communication, or other Wire or Electronic Communication within the definition of U.S. Hosting Data, is transmitted, which includes all records or other information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c)(1) and (d).

1.32. "United States" 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, thereby specifically including the territory of Guam.

1.33. "U.S. Hosting Data" means all data, records, documents, or information (including Domestic Communications, other Wire or Electronic Communications, CPNI, Subscriber Information, and Transactional Data) in any form (including but not limited to paper, electronic, magnetic, mechanical, or photographic) transmitted, received, generated, maintained, processed, used by or stored in a Data Center for a U.S. Hosting Services Customer.

1.34. "U.S. Hosting Services Customer" means any customer or subscriber that receives Hosting Services from the Domestic Communications Companies that is U.S.-domiciled or holds itself out as being U.S.-domiciled.

1.35. "USG Customer Information" means any Identifying Information for any U.S. Government customer of the Domestic Communications Companies as well as any other records or information pertaining to telecommunications equipment needs and/or purchases by any U.S. Government.

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

1.37. Other Definitional Provisions. Other capitalized terms used in this Agreement, including in the Preamble, 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: FACILITIES, INFORMATION STORAGE, AND ACCESS

2.1. Domestic Communications Infrastructure. Except to the extent and under conditions to which the USG Parties concur in writing:

(i) All Domestic Communications Infrastructure that is owned, operated, or controlled by the Domestic Communications Companies shall at all times be located in the United States and will be directed, controlled, supervised and managed by the Domestic Communications Companies.

(ii) All Domestic Communications that are carried by or through, in whole or in part, the Domestic Communications Infrastructure shall pass through a facility under the control of the Domestic Communications Companies and physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. The Domestic Communications Companies will provide technical or other assistance to facilitate such Electronic Surveillance.

(iii) Foreign connections to the Domestic Communications Companies' network shall be on a gateway basis using industry best practices, including that both signaling and traffic shall be monitored for unauthorized Access, network intrusions, and other malicious activity.

2.2. Data Centers and Access to Communications. Except to the extent and under conditions to which the USG Parties concur in writing:

(i) all Data Centers used to provide Hosting Services to U.S. Hosting Services Customers shall at all times be located in the United States; and

(ii) the Domestic Communications Companies shall, upon service of appropriate Lawful U.S. Process, ensure that Wire or Electronic Communications of a specified U.S. Hosting Services Customer that are transmitted to, from or through a Data Center shall be accessible from or pass through a facility under the control of the Domestic Communications Companies and physically located in the United States, from which Electronic Surveillance can be conducted in a timely manner. The Domestic Communications Companies will provide technical or other assistance to facilitate such Electronic Surveillance.

2.3. Network Operations Centers. Except to the extent and under conditions to which the USG Parties concur in writing:

(i) The Domestic Communications Companies agree to adopt (or cause the adoption of) security measures for the Domestic Communications Companies' NOCs that are consistent with, and based upon, the applicable security policies outlined in Section 3.1.

(ii) Network Management Information regarding the Domestic Communications Companies' NOC will be accessible only to persons who have been screened pursuant to Section 3.11 or the employee screening provisions in the security plan for the Domestic Communications Companies' NOC.

(iii) The current Domestic Communications Companies' NOC (or network functionalities of the current Domestic Communications Companies) shall at all times be located in the United States and will be directed, controlled, supervised and managed by the Domestic Communications Companies.

2.4. Information Storage. The Domestic Communications Companies shall store the following exclusively in the United States:

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

(ii) Wire Communications or Electronic Communications (including any other type of wire, voice or electronic communication not covered by the definitions of Wire Communication or Electronic Communication) received by, intended to be received by, or stored in the account of a customer or subscriber of the Domestic Communications Companies, if such communications are stored by or on behalf of the Domestic Communications Companies for any reason;

(iii) Transactional Data and Call Associated Data relating to Domestic Communications, if such data are stored by or on behalf of the Domestic Communications Companies for any reason;

(iv) CPNI and Subscriber Information, if such information is stored by or on behalf of the Domestic Communications Companies for any reason, concerning customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication;

(v) Billing records of customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication, for so long as such records are kept and at a minimum for as long as such records are required to be kept pursuant to applicable U.S. law or this Agreement;

(vi) Billing records as described in section 2.4(v) above shall be stored for at least five (5) years;

(vii) Network Management Information;

(viii) Classified Information and Sensitive Information.

2.5. Notice of Interconnection Agreement. The Domestic Communications Companies will notify the USG Parties of any Interconnection Agreement no later than thirty (30) days prior to the implementation of such agreement.

2.6. CPNI. Domestic Communications Companies shall comply, with respect to Domestic Communications, with all applicable FCC rules and regulations governing access to and storage of Customer Proprietary Network Information ("CPNI"), as defined in 47 U.S.C. § 222(h)(1).

2.7. Network Architecture and Principal Equipment. No later than thirty (30) days after the Effective Date of this Agreement, the Domestic Communications Companies shall provide to the USG Parties a comprehensive description of the Domestic Communications Companies' Domestic Communications Infrastructure to include the type and location of servers, routers, gateways, switches, operational systems software, and network security appliances and software, specifically regarding a description of the plans, processes, and procedures relating to network management operations, that secure the Domestic Communications Infrastructure from Access from outside the United States. The Domestic Communications Companies shall provide updates to such descriptions upon request of any of the USG Parties.

2.8. 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 in the United States to preserve any information in the possession, custody, or control of Domestic Communications Companies that is enumerated in Section 2.4 above, or any U.S. Hosting Data, Domestic Communications Companies shall store such information or such U.S. Hosting Data in the United States.

2.9. Compliance with Lawful U.S. Process. Domestic Communications Companies shall take all practicable steps to configure their Domestic Communications Infrastructure and Data Centers (except for equipment that is owned or controlled by a U.S. Hosting Services Customer and is collocated in the Domestic Communications Companies'-controlled space in a Data Center) to be capable of complying, and the Domestic Communications Companies' employees in the United States shall have authority to comply, in an effective, efficient, and unimpeded fashion, with:

(i) Lawful U.S. Process;

(ii) Telecommunications equipment facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications will have a CALEA solution.

ARTICLE 3: SECURITY

3.1. Security Policy. The Domestic Communications Companies shall adopt internal security policies and processes to ensure compliance with the Agreement and prevent Security Incidents. The Domestic Communications Companies shall include such measures in a Security Policy document that will be provided to the USG Parties for review and opportunity to comment no later than ninety (90) days after the Effective Date of this Agreement. The USG Parties will have thirty (30) days following submission of the Security Policy or any subsequent changes thereto to comment or object. If there is no objection, the Security Policy may take effect. Once effective, the Domestic

Communications Companies agree to provide the USG Parties written notice of any changes to the Security Policy as soon as reasonably practicable before such changes take effect, after which the USG Parties will have (30) thirty days to comment or object to such changes. This security policies document should be reviewed on an annual basis, and updated accordingly to ensure compliance with the Agreement as services and technologies change within the Domestic Communications Companies' enterprise architecture.

3.2. Security Officer Appointment, Responsibilities and Duties. The Head of Security of the Domestic Communications Companies, or a designee in a direct reporting relationship with the Head of Security, shall serve as the Security Officer with the primary responsibility for ensuring compliance with the Domestic Communications Companies' obligations under this Agreement. The Security Officer shall be a resident citizen of the United States (not a dual citizen) with an active security clearance or be eligible to apply for a security clearance. The Security Officer shall have the appropriate qualifications, authority, and resources within the company in order to ensure compliance with the Agreement. The Domestic Communications Companies will ensure that the Security Officer cooperates with any request by a USG Party for obtaining a security clearance or further background checks. No later than thirty (30) days after the Effective Date, the Domestic Communications Companies shall notify the USG Parties of the identity of the Security Officer, after which the USG Parties will have (30) thirty days to comment or object to the Domestic Communications Companies' selection of the Security Officer becoming effective.

3.3. Visitation Policy. As part of the Security Policy, the Domestic Communications Companies shall adopt and implement a visitation policy for all visits to Domestic Communications Infrastructure by Foreign Persons other than employees of the Domestic Communications Companies who have been screened pursuant to the procedures set forth in this Agreement. The visitation policy shall differentiate between categories of visits based on the sensitivity of the information, equipment, and personnel to which the visitors will have Access, and shall include a Routine Business Visit exception, as defined below. Under the policy, a written request for approval of a visit must be submitted to the Security Officer no less than seven (7) days prior to the date of the proposed visit. If a written request cannot be provided within seven (7) days of the proposed visit because of an unforeseen exigency, the request may be communicated via telephone to the Security Officer and immediately confirmed in writing; however, the Security Officer may refuse to accept any request submitted less than seven (7) days prior to the date of such proposed visit if the Security Officer determines that there is insufficient time to consider the request. For all visits to Domestic Communications Infrastructure covered by the Policy, the Security Officer shall review and approve or disapprove the requests. A record of all such visit requests, including the decision to approve or disapprove, and information regarding consummated visits, such as date and place, as well as the names, business affiliation and dates of birth of the visitors, and the Domestic Communications Companies' personnel involved shall be maintained by the Security Officer for 2 years. During all such visits, visitors will be escorted at all times by an employee, and under such conditions set forth by the Security Officer.

3.4. Routine Business Visits. Routine Business Visits by Foreign Persons may occur without prior approval by the Security Officer. A record of Routine Business Visits, including a log that contains the names of the visitors, their business affiliations, and the purpose of their visits, shall be maintained by the Security Officer for a period of at least two (2) years from the date of the visit itself. "Routine Business Visits" are those that: (a) are made in connection with the regular day-to-day business operations of the Domestic Communications Companies; (b) do not involve Access to Call Associated Data, Classified Information, CPNI, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information; and (c) pertain only to the commercial aspects of the Domestic Communications Companies' business. These may include, but not limited to:

(i) visits for the purpose of discussing or reviewing such commercial subjects as company performance versus plans or budgets; inventory, accounts receivable, accounting and financial controls; and business plans and implementation of business plans;

(ii) visits of the kind made by customers or commercial suppliers in general regarding the solicitation of orders, the quotation of prices, or the provision of products and services on a commercial basis; and

(iii) visits concerning fiscal, financial, or legal matters involving the Domestic Communications Companies.

Provided, however, that the obligations set forth in Sections 3.3 and 3.4 and the policies adopted thereto shall not apply to prospective and existing customer visits to Domestic Communications Companies' offices, retail stores, and outlets and the like for purposes of subscribing to or modifying services, paying bills, or otherwise managing their account with a Domestic Communications Company.

3.5. Information Security Policy. As part of the Security Policy, the Domestic Communications Companies shall develop, document, implement, and maintain an information security policy to:

(i) reflect information storage requirements within Section 2.4 and 2.6;

(ii) maintain appropriately secure facilities (e.g., offices) within the United States for the handling and storage of any Classified or Sensitive Information;

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

(iv) assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.11;

(v) upon request from the any of the USG Parties, provide the name, social security number and date of birth of each person who regularly handles or deals with Sensitive Information;

(vi) require that personnel handling Classified Information shall have been granted appropriate security clearances;

(vii) provide that the points of contact described in Section 3.10 of this Agreement shall have sufficient authority over any Domestic Communications Companies' employees who may handle Classified Information or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;

(viii) ensure that the disclosure of or Access to Classified Information or Sensitive Information is limited to those with a need to know, and who have the appropriate security clearances and authority.

3.6. Access by Foreign Government Authority. The Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to Call Associated Data, Classified Information, CPNI, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information stored by Domestic Communications Companies 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 the USG Parties or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Agreement shall be reported to the USG Parties as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the Security Officer. Domestic Communications Companies shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process.

3.7. Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities. Within thirty (30) days of receipt, the Domestic Communications Companies shall notify the USG Parties in writing of legal process or requests by foreign non-governmental entities to Domestic Communications Companies for Access to or disclosure of (i) U.S. Hosting Data, or (ii) Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure other than call data and other information exchanged in the ordinary course among interconnecting carriers and unless the disclosure of the legal process or request would be in violation of an order of a court of competent jurisdiction within the United States. In no event shall the Domestic Communications Companies fulfill any such requests prior to complying with this Section 3.7.

3.8. Restrictions on Access to Electronic Surveillance Information and Equipment, Lawful U.S. Process. The Security Officer will limit access to any information related to Electronic Surveillance activities or equipment or to Lawful U.S. Process, including but not limited to all Title III and Foreign Intelligence Surveillance Act (FISA) related intercepts, orders data and equipment. Specifically, unless otherwise agreed by the USG Parties or the agent of the USG who supplied the information to the Domestic Communications Companies, the Security Officer will ensure that only U.S. citizens with a need to know have access to such information and will control access to documents and systems in order to ensure the requisite limitations. The Security Officer will promptly

report to the USG Parties any attempt to access the information above or interfere with any Lawfully Authorized Electronic Surveillance activities, in a manner that is inconsistent with the requirements of this Agreement. The Security Officer will maintain a list of the identities of individuals to whom he has provided access to any Electronic Surveillance activities or equipment or to Lawful U.S. Process, and will produce such list upon request by a USG Party or its designee.

3.9. Removal of Security Officer. The Security Officer may be removed for any reason permitted by the provisions of applicable law or under the charter of the Domestic Communications Companies, provided that:

(i) the removal of the Security Officer shall not become effective until the USG Parties have received written notification of removal; a successor who is qualified within the terms of this Agreement is selected; the USG Parties receive written notice of the proposed replacement; and the USG Parties do not object to the proposed replacement within fifteen (15) days of receipt of such notice; and

(ii) notwithstanding the foregoing, however, if immediate removal of the Security Officer is deemed necessary to prevent actual or potential violation of any statute or regulation or actual or possible damage to the Domestic Communications Companies, the individual may be temporarily suspended, pending written notification to the USG Parties, and may be removed or reinstated under such time limits and conditions described in (i).

(iii) The Domestic Communications Companies shall not maintain a vacancy or suspension for the position of Security Officer for a period of more than sixty (60) days before Domestic Communications Companies nominate a qualified candidate to fill such vacancy, or terminate the suspension.

3.10. Point of Contact for Lawful U.S. Process. Within thirty (30) days after the Effective Date, the Domestic Communications Companies shall designate in writing to the USG Parties at least one nominee already holding a U.S. security clearance, or eligible for such a clearance, to serve as a primary point of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The point of contact shall be assigned to the Domestic Communications Companies' office(s) in the United States, shall be available twenty-four hours per day, seven days per week, and shall be responsible for accepting service and maintaining the security of Classified and Sensitive Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. The Domestic Communications Companies shall promptly notify the USG Parties of any change in such designation. The Domestic Communications Companies shall cooperate with any request by a U.S. federal, state, or local government entity within the United States that a further background check or further security clearance process be completed for a designated point of contact.

3.11. Screening of Personnel. The Domestic Communications Companies shall implement a thorough screening process as part of the Security Policy to ensure compliance with all personnel screening requirements agreed to by the Domestic Communications

Companies and the USG Parties, which includes screening for any existing or newly hired personnel (such personnel, upon completion of screening procedures, to be considered "Screened Personnel"):

(i) whose position involves Access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage), including those whose position involves system level privileges to Operations Support System (OSS) products, will be screened pursuant to Section 3.12 or the employee screening provisions in the security for the Domestic Communications Companies' NOC.

(ii) whose position allows Access to Call Associated Data, Classified Information, CPNI, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information;

(iii) all persons who have access to Sensitive Information or USG Facilities or premises;

(iv) all security personnel; and

(v) other personnel as deemed appropriate by the USG Parties.

3.12. Screening Process Requirements. Screening undertaken pursuant to this Article shall specifically include a background and financial investigation, in addition to a criminal records check.

(i) The Domestic Communications Companies shall provide the USG Parties an opportunity to comment on and object to their screening procedures. The Domestic Communications Companies shall utilize the criteria identified pursuant to Section 3.11 of this Agreement to screen personnel, shall report the results of such screening on a regular basis to the Security Officer, and shall, upon request, provide to the USG Parties all the information they collects in their screening process of each candidate. Candidates for these positions shall be informed that the information collected during the screening process may be provided to the U.S. Government, and the candidates shall consent to the sharing of this information with the U.S. Government.

(ii) The Domestic Communications Companies will cooperate with a request by the USG Parties or any U.S. Government agency desiring to conduct any further background checks. Individuals who the USG Parties' further background checks identify to the Domestic Communications Companies as posing a security concern shall not be hired or, if they have begun their employment, shall be immediately removed from their positions, or otherwise have their duties immediately modified so that they are no longer performing a function that would require screening under this Section.

(iii) The Domestic Communications Companies will notify the USG Parties of the transfer, departure, or job modification of any individual rejected from a position requiring screening because of the screening conducted pursuant to this Agreement within seven (7) days of such transfer or departure, and shall provide

the USG Parties with the name, date of birth and social security number of such individual.

(iv) The Domestic Communications Companies shall provide training programs to instruct Screened Personnel as to their obligations under the Agreement and the maintenance of their trustworthiness determination or requirements otherwise agreed. The Domestic Communications Companies shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.

(v) The Domestic Communications Companies shall maintain records relating to the status of Screened Personnel, and shall provide these records, upon request, to any or all of the USG Parties.

3.13. Notice of Obligations. The Domestic Communications Companies shall instruct appropriate officials, employees, contractors, and agents as to the security restrictions and safeguards imposed by this Agreement. Records of such instructions shall be maintained by the Security Officer.

3.14. Security Meetings with the U.S. Government. Upon request by any or all of the USG Parties, the Domestic Communications Companies shall meet with the requesting USG Parties and any other U.S. Government entity designated by the USG Parties, at any domestic company location, to discuss matters concerning the Companies' compliance with and enforcement of this Agreement and any other issue that could affect U.S. national security. The USG Parties shall coordinate such meetings and take reasonable steps so as not to place an undue economic burden on the Companies.

3.15. U.S. Government Access to Facilities, Records and Personnel. For the purpose of enforcement of compliance with this Agreement, including but not limited to conducting an audit pursuant to Section 6.7, upon forty-eight (48) hours prior written request from the USG Parties, including proof of Lawful U.S. Process where such request seeks Call Associated Data, CPNI, Subscriber Information, Access to Domestic Communications, Transactional Data, U.S. Hosting Data, or other information to be used for Electronic Surveillance or other purposes requiring Lawful U.S. Process, the Domestic Communication Companies shall provide access to all records requested, physical access to any company facilities, and access to personnel requested. The Companies may request a meeting to discuss the scope of the U.S. Government agency's request or other reasonable concerns, and the U.S. Government agency shall meet with the Companies as soon as possible, but the meeting request shall not excuse the Domestic Communications Companies' obligation to comply within the forty-eight hours.

ARTICLE 4. FACILITATING DEFENSE CONTRACTING ACTIVITIES

4.1. Except in emergency circumstances, should any of the Domestic Communications Companies' employees require regular access to any DOD restricted or controlled area(s) to initiate or maintain service (such areas to have been previously identified to the Companies' Security Officer), the Domestic Communications Companies agree to provide each employee's identification information, including the full name, Social

Security number (or equivalent residency authorization documentation number), as well as date and place of birth, to DOD thirty (30) days prior to seeking initial entry to those locations.

4.2. After the Security Officer has been advised that DOD is the direct customer of another communications carrier, before terminating any existing access, interconnection, peering, or resale arrangement with that carrier, the Companies will provide notice to DOD allowing thirty (30) days for DOD to respond prior to such termination.

4.3. The Companies understand the DOD may need to realign their activities in the future. The Domestic Communications Companies' business, engineering, and technical staff will participate in coordination with DOD representatives for planning and implementation purposes, and will promptly provide necessarily technical data to support the DOD operational needs. Upon written request, the Companies will meet and confer with any US government official designed by the DOD to address any concerns with respect to these matters.

ARTICLE 5: DISPUTES AND REMEDIES

5.1. Informal Resolution. The Parties shall use their best efforts to resolve any disagreements or incidents that may arise under this Agreement. Disagreements or incidents 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 policy-level officials of the USG Parties, unless those higher authorized officials believe that important national interests can be protected, or the Companies believe that their paramount commercial interests can be resolved, only by resorting to the measures set forth in this Agreement. 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 this Agreement.

5.2. Enforcement of Agreement. If any of the Parties believes that any other of the Parties has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate injunctive or other judicial relief. Nothing in this Agreement shall limit or affect the right of any Party to exercise any rights it may have under law or regulation or this Agreement. In the case of the USG Parties, this includes, but is not limited to, any or all of the following:

(i) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty days upon receiving written notice of such breach;

(ii) require that the Domestic Communications Companies pay monetary damages and reasonable costs associated with compensating the USG Parties for actual and direct expenses associated with an incident of breach; provided, however, that

nothing in this provision shall require the Domestic Communications Companies to compensate the USG Parties for any indirect or consequential damages;

(iii) seek civil remedies for any violation by the Domestic Communications Companies of any U.S. law or regulation or term of this Agreement;

(iv) pursue criminal sanctions against the Domestic Communications Companies, or any director, officer, employee, representative, or agent of the Domestic Communications Companies, or against any other person or entity, for violations of the criminal laws of the United States; or

(v) seek suspension or debarment of the Domestic Communications Companies from eligibility for contracting with the U.S. Government.

5.3 Security Incidents. The Parties agree that if any Personnel of the Companies knowingly uses or participates in the use of the Domestic Communications Companies' services or products in any Security Incident, this shall constitute a breach of this Agreement.

5.4 Indemnification of Security Officer. The Companies shall indemnify and hold harmless the Security Officer of the Domestic Communications Companies from any and all claims arising from, or in any way connected to, his or her performance as Security Officer under this Agreement. The Companies shall advance fees and costs incurred in connection with the defense of such claim.

5.5 Non-Waiver of Third Party Claims. Nothing contained in this Article shall be deemed a waiver of any claims or remedies the Domestic Communications Companies may have against third parties related to this Agreement.

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

ARTICLE 6: REPORTING, NOTICE AND LIMITS

6.1. Outsourcing. The Domestic Communications Companies shall not outsource functions covered by this Agreement, except pursuant to an outsourcing policy to be reviewed by the USG Parties. Such policy shall include prior notice of the proposed outsourcing and the right of the USG Parties to object within thirty (30) days of receipt of notice to the proposed outsourcing. The parties agree to exclude from this notice and approval requirement outsourcing contracts that do not provide Access to Call Associated Data, Classified Information, CPNI, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information. Further:

(i) the Domestic Communications Companies shall ensure that the entity complies with the applicable terms of this Agreement;

(ii) the Domestic Communications Companies shall include in their contracts with any such entities written provisions requiring that such entities comply with all applicable terms of this Agreement (and otherwise ensure that such entities are aware of, agree to, and are bound to comply with the applicable obligations of this Agreement);

(iii) if the Domestic Communications Companies are reasonably uncertain as to whether an outsourcing contract is covered by the outsourcing policy, they shall include in the contract a provision that such contract may be terminated should the USG Parties object to the contract, shall notify the USG Parties within thirty (30) days of executing the contract, which notice shall identify the name of the entity and the nature of the contract, and the USG Parties shall have thirty (30) days from notice in which to object to the outsourcing contract;

(iv) if the Domestic Communications Companies learn that the entity or the entity's employee has violated an applicable provision of this Agreement, the Domestic Communications Companies will notify the USG Parties promptly; and

(v) with consultation and, as appropriate, cooperation with the USG Parties, the Domestic Communications Companies will take reasonable steps necessary to rectify promptly the situation, which steps may (among others) include terminating the arrangement with the entity, including after notice and opportunity for cure, and/or initiating and pursuing litigation or other remedies at law and equity.

Peering, interconnection and purchase of local access service shall not constitute outsourced functions for purposes of this Agreement.

6.2. Joint Ventures. The Domestic Communications Companies may have entered into or may enter into joint ventures under which the joint venture or entity may provide Domestic Communications.

(i) To the extent that such Domestic Communications Companies do not have de facto or de jure control over a joint venture or entity, such Domestic Communications Companies shall in good faith (a) notify such entity of this Agreement and its purposes, (b) endeavor to have such entity comply with this Agreement as if it were a Domestic Communications Company, and (c) consult with the USG Parties about the activities of such entity. Nothing in this section shall be construed to relieve Domestic Communications Companies of obligations under Article 2 of this Agreement.

(ii) If the Domestic Communications Companies enter into a joint venture under which the joint venture or entity may provide Domestic Communications or transmission, switching, bridging, routing equipment (including software and upgrades), facilities used to provide, process, direct, control, supervise or manage Domestic Communications, the Domestic Communications Companies must provide the USG Parties with notice no later than 30 days before the joint venture offers Domestic Communications service. The USG Parties will have 30 days

from receipt of the notice to review and provide the Domestic Communications Companies with any objection to the joint venture. Any objection shall be based on national security, law enforcement or public safety grounds. If the USG Parties object, the joint venture shall not offer Domestic Communications service.

6.3. Notice of Foreign Influence. If any member of the senior management of the Domestic Communications Companies (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer, Head of Network Operations, Head of Security, Security Officer, or other such senior officer) acquire any information that reasonably indicates that any Foreign Person has acted or plans to act in any way that interferes with or impedes the performance by the Domestic Communications Companies of their duties and obligations under the terms of this Agreement, or the exercise by the Domestic Communications Companies of their rights under this Agreement, then such member shall promptly notify the Security Officer, who in turn shall promptly, and in any event, no later than five (5) days from the reasonable indication of such actions or plans, notify the USG Parties in writing of the timing and the nature of the foreign government's or entity's actions or plans.

6.4. Reporting of Incidents. The Domestic Communications Companies shall take practicable steps to ensure that, if any of their officer, director, employee, contractor or agent acquire any information that reasonably indicates: (a) a breach of this Agreement; (b) Access to or disclosure of U.S. Hosting Data or 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 Information or Sensitive Information, then the individual will notify the Security Officer, who will in turn notify the USG Parties within five (5) days. This report shall be made promptly and in any event no later than five (5) calendar days after the Domestic Communications Companies acquire information indicating a matter described above. The Domestic Communications Companies shall lawfully cooperate in investigating the matters described in this Section of this Agreement. The Domestic Communications Companies 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.

6.5. Non-Retaliation. The Domestic Communications Companies shall, by duly authorized action of their respective boards of directors, adopt and distribute an official corporate policy that strictly prohibits any of the Domestic Communications Companies 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 Sections 6.3 and 6.4 of this Agreement, or has notified or attempted to notify directly the Security Officer named in the policy to convey information that he or she believes in good faith would be required to be reported to the USG Parties by the Security Officer under Sections 6.3, and 6.4 of this Agreement. Such corporate policy shall set forth in a clear and prominent manner the contact information for the Security Officer to whom such contacts may be made directly by any officer,

director, employee, contractor or agent for the purpose of such report or notification. Any violation by the Domestic Communications Companies of any material term of such corporate policy shall constitute a breach of this Agreement.

6.6. Annual Report. On or before the last day of January of each year, the Security Officer shall submit to the USG Parties a report assessing Domestic Communications Companies' compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

(i) a certification of compliance with this agreement, signed by the Security Officer;

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

(iii) a summary of any known acts of material 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

(iv) identification of any other issues that, to Domestic Communications Companies' knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement. The Domestic Communications Companies shall make available to the Security Officer, in a timely fashion, all information necessary to complete the report required by this Section.

6.7. Third Party Network Security Audits. The Domestic Communications Companies shall retain and pay for a neutral third party telecommunications engineer to audit their operations objectively on an annual basis. The Domestic Communications Companies shall provide notice of their selected auditor to the USG Parties, and the USG Parties shall be able to review and object to the selected auditor and terms of reference for that auditor within thirty days of receiving notice. In addition, the Domestic Communications Companies shall provide to the USG Parties a copy of their contract with the third party auditor, which shall include terms defining the scope and purpose of the audits. The USG Parties shall have the right to review and comment on the terms defining the scope and purpose of the audits. Through their contract with the third party auditor, the Domestic Communications Companies shall ensure that all reports generated by the auditor are provided promptly to the USG Parties. The Domestic Communications Companies also will provide the USG Parties with access to facilities, information, and personnel consistent with Section 3.15 in the event that the USG Parties wish to conduct their own audit of the Domestic Communications Companies. The terms defining the scope and purpose of the audits shall include, at a minimum, the following:

(i) Development of an initial vulnerability and risk assessment based on this Agreement, and a detailed audit work plan based on such assessment, which work plan may, at the discretion of the USG Parties, be subject to review and approval by the USG Parties;

(ii) Authority for the auditor to review and analyze the Domestic Communications Companies' security policies and procedures related to network security;

(iii) Authority to audit the integrity of password systems, review access logs, review logs regarding any access to a capability to conduct electronic surveillance, conduct switch audits to discover "Free Line Service" accounts;

(iv) Authority for the auditor to review and analyze relevant information related to the configuration of the Domestic Communications Companies' network;

(v) Authority for the auditor to conduct a reasonable number of unannounced inspections of the Domestic Communications Companies facilities;

(vi) Authority for the auditor to conduct a reasonable volume of random testing of network firewalls, access points and other systems for potential vulnerabilities;

(vii) Other authorities related to network security as agreed by the parties after consultation with the USG Parties.

6.8. Information and Reports Concerning Network Architecture. The Domestic Communications Companies shall provide to the USG Parties, on an annual basis, the following information regarding the interconnections and control of the Domestic Communications Infrastructure:

(i) A description of the plans, processes and/or procedures, relating to network management that prevent the Domestic Communications Infrastructure from being accessed or controlled from outside the United States.

(ii) A description of the placement of Network Operations Centers and interconnection (for service offload or administrative activities) to other domestic and international carriers, ISPs and critical U.S. financial, energy, and transportation infrastructures.

(iii) A description of the Domestic Communications Companies' IP and transport networks and operations processes, procedures for management control and relation to the backbone infrastructures of other service providers.

(iv) A description of any unique or proprietary control mechanisms of the Domestic Communications Companies' operating and administrative software.

(v) A report of Network Management Information that includes an assurance that network performance satisfies FCC rules and reporting requirements.

(vi) A description of the placement of data centers that host system software, application software, and utilities for managing the Domestic Communications Companies' telecommunication networks.

The Domestic Communications Companies shall promptly report any material changes, upgrades and/or modifications to the items described in (i) - (v) above, including the installation of critical equipment and software. For the purposes of this section, critical equipment and software shall include: routers, switches, gateways, network security appliances, network management/test equipment, operating systems and network and security software (including new versions, patches, upgrades, and replacement software), and other hardware, software, or systems performing similar functions. Monitors, desktop computers, desktop computer applications, disk drives, power supplies, printers, racks and the like are not "critical equipment or software" unless they perform functions

similar to those of the items described in (i) - (v) above. Similarly, "material" for the purposes of this paragraph shall refer to those changes, modifications and upgrades that alter network operating characteristics or architecture--it does not apply to spare parts replacement, the one-for-one swapping of identical equipment or the related re-loading of system software or backups--provided, however, that network security configuration and capabilities remain unchanged.

6.9. Control of the Domestic Communications Companies. If any member of the senior management of the Domestic Communications Companies (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer, Head of Network Operations, Head of Security, Security Officer, or other senior officer) acquires any information that reasonably indicates that any single foreign entity or individual, other than funds serviced by Advantage Partners, LLP and their affiliates has obtained or will likely obtain an ownership interest (direct or indirect) in the Domestic Communications Companies above ten (10) percent, as determined in accordance with 47 C.F.R. § 63.09, or if any single foreign entity or individual has gained or will likely otherwise gain either (1) Control or (2) *de facto* or *de jure* control of the Domestic Communications Companies, then such member shall promptly cause to be notified the Security Officer, who in turn, shall promptly, and in any event, no later than ten (10) days, notify the USG Parties of such information in writing. Notice under this section shall, at a minimum:

(i) Identify the entity or individual(s) (specifying the name, addresses, email, and telephone numbers of the entity);

(ii) Identify the beneficial owners of the increased or prospective increased interest in the Domestic Communications Companies by the entity or individual(s) (specifying the name, addresses, emails, and telephone numbers of each beneficial owner); and

(iii) Quantify the amount of ownership interest in a Domestic Communications Company that has resulted in or will likely result in the entity or individual(s) increasing the ownership interest in or control of the Domestic Communications Companies.

ARTICLE 7: FREEDOM OF INFORMATION ACT

7.1. FOIA Confidentiality. If so marked by the Companies, information supplied to the USG Parties by the Companies pursuant to the terms of this Agreement as containing proprietary, trade secret, commercial, or financial information, and voluntarily provided pursuant to a request for confidentiality, will be treated by the USG Parties as exempt from disclosure under the Freedom of Information Act (5 U.S.C. § 552) under Exemption (b)(4).

ARTICLE 8: FCC CONDITION

8.1 FCC Approval. Upon execution of this Agreement by all the Parties, the USG Parties shall promptly notify the FCC that, provided the FCC adopts a condition substantially the

same as set forth in Appendix A to this Agreement, the DOD, DOJ and DHS have no objection to the grant of the Domestic Communications Companies' Petition for Declaratory Ruling and applications filed with the FCC as reflected in WT Docket No. 10-260. This Section 8.1 is effective upon the Effective Date.

ARTICLE 9: MISCELLANEOUS PROVISIONS

9.1 Obligations. The Domestic Communications Companies jointly and severally shall comply with this Agreement and, where appropriate, may act through GTA TeleGuam or subsidiaries to discharge their obligations under this Agreement.

9.2 Corporate Structure. Within ninety (90) days of the Effective Date, the Domestic Communications Companies shall provide to the USG Parties a description of the contemplated corporate structure of the Companies as it relates to the Domestic Communications Companies' ownership and control, including the placement of the subsidiaries within the corporate structure that will be in effect as of the Effective Date, which description shall be included as Appendix B to this Agreement. The description shall identify the parent company or companies of each of the Domestic Communications Companies and the subsidiaries in the Corporate Structure. Following the Effective Date, the Domestic Communications Companies shall notify the USG Parties prior to any modification of the companies' corporate structure and shall provide an updated description, which shall be incorporated into Appendix B; provided that if a modification to the Corporate Structure does not change the entity that Controls the Domestic Communications Companies, then they shall notify the USG Parties of the change within thirty (30) days after consummation of the change, which shall be incorporated into Appendix B.

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

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

9.5 Other Laws. Nothing in this Agreement is intended to limit or alter or constitute a waiver of (a) any obligation imposed on the Domestic Communications Companies, their Personnel, or their agents by any U.S. federal, state or local laws, (b) any enforcement authority available under any U.S. federal, state, or local laws, (c) the sovereign immunity of the United States, (d) any authority or jurisdiction the U.S. Government may possess over the activities of the Domestic Communications Companies, their Personnel, or their agents located within or outside the United States, or (e) any rights of the Domestic Communications Companies, their Personnel, or their agents under the U.S. Constitution, any state constitution, or any U.S. federal, state, or local laws. Nothing in this Agreement is intended to or is to be interpreted to require the Domestic

Communications Companies, their Personnel, or the USG Parties to violate any applicable U.S. law. Likewise, nothing in this Agreement limits the right of the U.S. Government to pursue criminal or civil sanctions or charges against the Domestic Communications Companies or their Personnel in an appropriate case, and nothing in this Agreement provides the Domestic Communications Companies, their Personnel, or their agents with any relief from civil liability in an appropriate case.

9.6 Waiver. The taking of any action by a USG Party or other appropriate governmental authority in the exercise of any remedy shall not be considered a waiver by that USG Party or authority of any other rights or remedies. The failure of a USG Party to insist on strict performance of any of the provisions of this Agreement, or to exercise any right granted herein, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by any Party to any provision or right shall be valid unless it is in writing and signed by the Party.

9.7 Choice of Law. This Agreement shall be governed by and interpreted according to the laws of the District of Columbia.

9.8 Forum Selection. Any civil action among the Domestic Communications Companies and the USG 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 or the United States Court of Federal Claims.

9.9 Integrated Agreement. This Agreement and all appendices hereto is a fully integrated agreement.

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

9.11 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.

9.12 Modifications. This Agreement may only be modified by written agreement signed by all of the Parties.

9.13 Non-Parties. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties.

9.14 Changes in Circumstances for USG Parties. If, after the Effective Date, the USG Parties find that the terms of this Agreement are inadequate to address their national security concerns, then the Domestic Communications Companies will negotiate in good faith to modify this Agreement to address those concerns. In the event that improvements in technology may enhance the efficacy of this Agreement to protect the national

security, the Parties will negotiate promptly and in good faith to amend the Agreement to implement such advances.

9.15 Changes in Circumstances for Domestic Communications Companies. The USG Parties agree to negotiate in good faith and promptly with respect to any request by the Domestic Communications Companies for relief from application of specific provisions of this agreement: (a) if the Domestic Communications Companies provide Domestic Communications solely through the resale of transmission or switching facilities owned by third parties, or (b) as regards future Domestic Communications Company activities or services, if those provisions become unduly burdensome or adversely affect the Domestic Communications Companies' competitive position.

9.16 Termination. After the Effective Date, this Agreement may be terminated at any time by a written agreement signed by the Parties.

9.17. Termination of Merger Agreement. If the Merger Agreement is terminated prior to the Effective Date, the Domestic Communications Companies shall promptly provide written notification of such termination to the USG Parties, and upon receipt of such written notice, this Agreement shall automatically terminate.

9.18. 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.

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

9.20 Successors and Assigns. This Agreement shall inure to the benefit of and shall be binding upon the Parties and their respective successors and assigns; for purposes of this Agreement, successors and assigns under this Section shall include any corporate name changes.

9.22. Notices. As of the Effective Date, all notices and other communications given or made relating to this Agreement, such as a proposed modification, shall be in writing and shall be deemed to have been duly given or made as of the date of receipt and shall be sent by electronic mail and by one of the following means: (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, unless provided otherwise in this Agreement; provided, however, that upon written notification to the Parties, any party to this Agreement may unilaterally amend or modify its designated representative information, notwithstanding any provision to the contrary in this Agreement:

For the TeleGuam Entities:

Daniel G. Moffat
President and Chief Executive Officer
624 North Marine Corps Drive
Tamuning, Guam 96913
Tel: (671) 644-0000
Fax: (671) 644-0010
E-mail: dmoffat@gta.net

and Counsel for the TeleGuam Entities:

Andrew D. Lipman
Jean L. Kiddoo
Bingham McCutchen LLP
2020 K Street, N.W.
Washington, DC 20009-1806
Tel: (202) 373-6000
Fax: (202) 373-6001
E-mail: andrew.lipman@bingham.com
E-mail: jean.kiddoo@bingham.com

For AP TG, on behalf of itself and AP TeleGuam Merger Sub:

Stanley Emmett Thomas, III
Director
AP TeleGuam Holdings, Inc.
c/o 160 Greentree Drive, Suite 101
Dover, Delaware 19904
Tel: (302) 674-4089
E-mail: emmett.thomas@advantagepartners.com

and Counsel for AP TG and AP TeleGuam Merger Sub:

Laura L. Fraedrich
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, DC 20005-5793
Tel: (202) 879-5990
Fax: (202) 879-5200
E-mail: laura.fraedrich@kirkland.com

For the U.S. Department of Justice:

Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530
Tel: (202) 514-1057
Fax: (202) 353-9836
E-mail: TTelecom@usdoj.gov

For the U.S. Department of Homeland Security:

Office of the Assistant Secretary for Policy
U.S. Department of Homeland Security
NAC, Building 17-134
Anacostia Naval Annex, Bldg 410
245 Murray Lane, S.W.
Washington, DC 20528
Tel: (202) 447-3817
Fax: (202) 282-8503
E-mail: IP-FCC@DHS.GOV

For the U.S. Department of Defense:

Office of the Assistant Secretary of Defense for
Networks and Information Integration/ DoD Chief
Information Officer (ASD(NII)/DoD CIO) Trusted
Mission Systems and Networks (TMSN)
[ATTN: Transactional Risk Management (TRM) Team]
6000 Defense Pentagon, Room 3D1048
Washington, DC 20301-6000
E-mail: cfius.monitoring@osd.mil

and

Defense Information Systems Agency
General Counsel
[ATTN: D01/GC]
6910 Cooper Avenue
Fort Meade, Maryland 20755-7088
Tel: (301) 225-6113
Fax: (301) 225-0510
E-mail: generalcounseldisa@disa.mil

This Agreement is executed on behalf of the Parties:

Date: May ___, 2011

AP TeleGuam Holdings, Inc., on behalf of itself and AP TeleGuam Merger Sub, LLC

By:_____
Name:
Title:

Date: May ___, 2011

TeleGuam Holdings, LLC, on behalf of itself and GTA Telecom, LLC, GTA Services, LLC, and Pulse Mobile, LLC

By:_____
Name:
Title:

Date: May ___, 2011

United States Department of Justice

By:_____
Name:
Title:

Date: May ___, 2011

United States Department of Homeland Security

By:_____
Name:
Title:

Date: May ___, 2011

United States Department of Defense

By:_____
Name:
Title:

APPENDIX A

CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between AP TeleGuam Holdings, Inc., ("AP TG"),[3] on behalf of itself and AP TeleGuam Merger Sub, LLC, its wholly owned subsidiary created for purposes of the transaction subject to this Agreement through which AP TG will acquire TeleGuam Holdings, LLC, GTA Telecom, LLC, GTA Services, LLC, and Pulse Mobile, LLC, on the one hand, and the U.S. Department of Justice ("DOJ"), the U.S. Department of Homeland Security ("DHS"), and the U.S. Department of Defense ("DoD") on the other (collectively, "the USG Parties"), dated May ___, 2011, which Agreement is intended to enhance the protection of U.S. national security, law enforcement, and public safety. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation.

[3] At the time of the proposed closing, AP TG will be jointly owned by three private investment funds that will collectively own approximately 97.2 percent of the company: (1) Advantage Partners IV, ILP (an Investment Limited Partnership with Japan citizenship, 42.2 percent), (2) AP Cayman Partners II, L.P. (Cayman Islands citizenship, 29.4 percent), and (3) Japan Ireland Investment Partners (Ireland citizenship, 25.6 percent).

APPENDIX B

CORPORATE STRUCTURE