AGREEMENT

This AGREEMENT is made as of the date of the last signature affixed hereto by and between Guam Cellular and Paging, Inc. ("GC") and DoCoMo Guam Holdings, Inc. ("DCMG"), on the one hand, and the Federal Bureau of Investigation ("FBI"), the U.S. Department of Justice ("DOJ"), and the U.S. Department of Homeland Security ("DHS"), on the other (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 7, Critical Infrastructure Identification, Prioritization, and Protection);

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

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

WHEREAS, GC holds the cellular A block licenses in Guam and the Commonwealth of Northern Mariana Island ("CNMI"). GC also holds several other licenses in Guam and the CNMI, including paging, common carrier fixed point-to-point microwave, industrial/business pool, wireless communications service, and 700 MHz lower band licenses. In addition, GC holds two international Section 214 licenses authorizing it to provide international global resale and facilities-based telecommunications services pursuant to Section 214 of the Communications Act of 1934, as amended (the "Act"), 47 U.S.C. § 214. GC has provided high quality mobile wireless services, based upon the CDMA wireless standard, to residents of and visitors to Guam and the CNMI since 1992. GC also provides paging services, business and residential wireline domestic long distance and international (via direct dialing and calling card) services, and dial-up and DSL Internet access services. GC provides service under the brand names "Guamcell Communications" in Guam and "Saipancell Communications" in the CNMI.

WHEREAS, Guam Wireless Telephone Company L.L.C. ("Guam Wireless") holds a broadband Personal Communications Service ("PCS") B block license that serves Guam and the CNMI. Guam Wireless also holds an international Section 214 license pursuant to Section 214 of the Act authorizing it to provide international telecommunications services on a global resale and facilities basis. Guam Wireless provides high quality mobile wireless services under the brand name "HafaTEL" to residents of and visitors to Guam and the CNMI using the GSM wireless standard.

WHEREAS, GC is the subject of the Share Purchase Agreement among NTT DoCoMo, Inc. ("DCM"), GC, and GC's shareholders dated as of March 20, 2006 ("SPA");

WHEREAS, Guam Wireless is the subject to the Asset Purchase Agreement among DCM, Guam Wireless, and Guam Wireless' shareholders dated as of March 20, 2006 ("APA");

WHEREAS, DCM, GC and Guam Wireless have filed with the Federal Communications Commission ("FCC") applications (in FCC IB Docket No. 06-96) under Sections 214 and 310(d) of the Act, 47 U.S.C. §§ 214, 310(d), seeking FCC consent to assign and transfer of control Guam Wireless' and GC's licenses and requesting a declaratory ruling pursuant to Section 310(b)4 of the Act, 47 U.S.C. § 310(b)(4), that the proposed foreign ownership by DCMG is in the public interest;

WHEREAS, as disclosed to the FCC, DCMG is a corporation, organized and existing under the laws of the Guam, and which is a wholly-owned subsidiary of DCM, a Japanese corporation existing under the laws of the Japan;

WHEREAS, the FCC's grant of the applications in FCC IB Docket No. 06-96 may be made subject to conditions relating to national security, law enforcement, and public safety, and whereas GC and DCMG each have entered into this Agreement with the FBI, the DOJ, and the DHS to address issues raised by those departments and agencies, and to request that the FCC condition the assignment and transfer of control approved by the FCC on their compliance with this Agreement;

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 "APA" has the meaning given in the Recitals.

1.2. "Call Associated Data" means any information related to a Domestic Communication or related to the sender or recipient of that Domestic Communication and,

to the extent maintained by a Domestic Communications Company in the normal course of business, 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 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 any information that has been determined pursuant to Executive Order 12958, or any predecessor or successor order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.

1.4. "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:

(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 nonfulfillment 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;

or

(vi) GC's obligations under this Agreement.

1.5. "Controlled Unclassified Information" means unclassified information, the export of which is controlled by the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Chapter I, Subchapter M, or the Export Administration Regulations ("EAR"), 15 C.F.R., Chapter VII, Subchapter C.

1.6. "DCM" means NTT DoCoMo, Inc.

1.7. "DCMG" means DoCoMo Guam Holdings, Inc.

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

1.9. "DHS" means the U.S. Department of Homeland Security.

1.10. "DOJ" means the U.S. Department of Justice.

1.11. "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.

1.12. "Domestic Communications Company" means all those subsidiaries, divisions, departments, branches and other components of DCMG, and any other entity over which DCMG has *de facto* or *de jure* control, that provide Domestic Communications, including GC. If any subsidiary, division, department, branch or other component of DCMG, or any other entity over which DCMG has *de facto* or *de jure* control, provides Domestic Communications after the date that all the Parties execute this Agreement, then such entity shall be deemed to be a Domestic Communications Company. If any Domestic Communications Company enters into joint ventures under which a joint venture or another entity may provide Domestic Communications and if a Domestic Communications Company has the power or authority to exercise *de facto* or *de jure* control over such entity, then DCMG will ensure that that entity shall fully comply with the terms of this Agreement. The term "Domestic Communications Company" shall not include acquisitions by DCMG in the U.S. after the date that this Agreement is executed by all parties only if the DOJ or the FBI find that the terms of this Agreement are inadequate to address national security, law enforcement or public safety concerns presented by that acquisition and the necessary modifications to this Agreement cannot be reached pursuant to Section 8.6 below. Nothing in this definition shall exempt any Domestic Communications Company from its obligations under Section 5.3.

1.13. "Domestic Communications Infrastructure" means (a) transmission, switching, bridging and routing equipment (including software and upgrades) subject to control by and used by or on behalf of a Domestic Communications Company to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of a Domestic Communications Company that are physically located in the United States; and (c) facilities used by or on behalf of a Domestic Communications Company to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers other than Domestic Communications Companies that are: (a) interconnecting communications providers; or (b) providers of services or content that are (1) accessible using the communications services of Domestic Communications Companies, and (2) available in substantially similar form and on commercially reasonable terms through

communications services of companies other than Domestic Communications Companies. The phrase "on behalf of" as used in this Section does not include entities with which a Domestic Communications Company has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the parties may agree. 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 system in the United States.

1.14. "Effective Date" means the date on which the transactions contemplated by the SPA and APA are consummated.

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

1.16. "Electronic Surveillance" means: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(4), (1), (2), 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 or interception of, or preservation of communications or information as described in (a) through (e) above and comparable state laws.

1.17. "FBI" means the Federal Bureau of Investigation.

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

1.19. "GC" means Guam Cellular and Paging, Inc.

1.20. "Governmental Authority" or "Governmental 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.

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

1.22. "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, Call Associated Data, Transactional Data, or Subscriber Information.

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

1.24. "OPM" means the Office of Personnel Management of the U.S. Government.

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

1.26. "*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 the FCC's Rules.

1.27. "Share Purchase Agreement" has the meaning given in the Recitals.

1.28. "Security Officer" has the meaning given in Sections 3.10.

1.29. "Sensitive Information" means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance 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, (f) information deemed to be Sensitive Information pursuant to Executive Order, decision or guidelines, and (g) other information that is not Classified Information designated in writing by an authorized official of a Federal, state or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information." Domestic Communications Companies may dispute pursuant to Article 4 whether information is Sensitive Information under this subparagraph. Such information shall be treated as Sensitive Information unless and until the dispute is resolved in the Domestic Communications Companies' favor.

1.30. "Subscriber Information" means information relating to subscribers or customers of a Domestic Communications Company 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.

1.31. "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 a Domestic Communications Company 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, 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 (iii) below;

(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, including electronic mail headers showing From: and To: addresses; and

(iv) 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. The term 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), but does not include the content of any communication. The phrase "on behalf of" as used in this Section does not include entities with which a Domestic Communications Company has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the parties may agree.

1.32. "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, and specifically includes Guam and the Commonwealth of the Northern Mariana Islands.

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

1.34. 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: FACILITIES, INFORMATION STORAGE AND ACCESS

2.1. Domestic Communications Infrastructure. Except to the extent and under conditions concurred in by the FBI, DOJ and DHS in writing:

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

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

2.2. Compliance with Lawful U.S. Process. Domestic Communications Companies shall take all practicable steps to configure their Domestic Communications Infrastructure to be capable of complying, and Domestic Communications Company employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

(i) Lawful U.S. Process;

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

(iii) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Act , 47 U.S.C. § 151 et seq.

2.3. Information Storage and Access. Domestic Communications Companies, effective upon execution of this Agreement by all Parties, shall store exclusively in the United States the following:

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

(ii) any 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 a Domestic Communications Company, if such communications are stored by or on behalf of a Domestic Communications Company for any reason;

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

(iv) Subscriber Information, if such information is stored by or on behalf of a Domestic Communications Company 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; and

(vi) Network Management Information, provided, however, that a duplicate copy of such Network Management Information may be maintained at DCM's headquarters at Sanno Park Tower 2-11-1, Nagata-cho, Chiyoda-ku Tokyo 100-6150, Japan.

The phrase "on behalf of" as used in this Section does not include entities with which a Domestic Communications Company has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

2.4. Billing Records. Domestic Communications Companies shall store for at least 18 months all billing records described in Section 2.3(v) above. Nothing in this paragraph shall require Domestic Communications Companies to store such records for longer than 18 months.

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 Governmental Authority in the United States to preserve any information in the possession, custody, or control of Domestic Communications Companies that is enumerated in Section 2.3 above, Domestic Communications Companies shall store such information in the United States.

2.6. Compliance with U.S. Law. Nothing in this Agreement shall excuse a Domestic Communications Company from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of such information or data.

Similarly, in any action to enforce Lawful U.S. Process, Domestic Communications Companies have not waived any legal right they might have to resist such process.

2.7. Routing of Domestic Communications. Except for routing of traffic (i) from or to U.S. states, territories and possessions outside the Continental United States, (ii) to avoid network disruptions, (iii) consistent with least-cost routing practices and (iv) as otherwise may be agreed in writing by the DOJ, the FBI and the DHS, Domestic Communications Companies shall not route Domestic Communications outside the United States.

2.8. 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).

2.9. Storage of Protected Information. The storage of Classified, Controlled Unclassified, and Sensitive Information by a Domestic Communications Company or its contractors at any location outside of the United States is prohibited, unless the storage is at a U.S. military facility, a U.S. Embassy or Consulate or other location occupied by a U.S. government organization.

ARTICLE 3: SECURITY

3.1. Measures to Prevent Improper Use or Access. Domestic Communications Companies shall take all reasonable measures to prevent the use of or access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to obtain or disclose Domestic Communications, Classified Information, Sensitive Information, or Controlled Unclassified Information, in violation of any U.S. Federal, state, or local laws or the terms of this Agreement. These measures shall include creating and complying with detailed technical, organizational, operational, and personnel controls, policies and written procedures, necessary implementation plans, and physical security measures.

3.2. Visitation Policy. A Domestic Communications Company shall adopt and implement a visitation policy within ninety (90) days of the Effective Date. The policy shall apply to all visits by non-U.S. persons to Domestic Communications Infrastructure, except for Routine Business Visits, as defined in Section 3.3 below. A Domestic Communications Company shall consult with the DHS in the design and implementation of its visitation policy. The visitation policy shall require that:

(i) the Security Officer shall review and approve or disapprove requests for visits to Domestic Communications Infrastructure (provided that, with respect to carrier hotels and other shared facilities, this policy will apply solely to the portion of the facility controlled by a Domestic Communications Company) by all non-U.S. persons, organizations or entities ("Visits"). The Security Officer shall approve or disapprove Visit requests on the basis of

their consistency with the visitation policy; the Security Officer may specifically deny any Visit request on security or related grounds, which will be described more fully in the visitation policy.

(ii) 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.

(iii) each request shall set forth the exact purpose and justification for the Visit in sufficient detail to enable the Security Officer to make an informed decision concerning the appropriateness of the proposed visit. The Security Officer may refuse to accept any request that he or she believes lacks sufficient information. Each proposed Visit and each individual visitor must be justified and a separate approval request must be submitted for each visit, unless the Security Officer agrees to approve multiple visits by the same person or persons for the same purpose, for a period not to exceed sixty (60) days.

(iv) the Security Officer shall evaluate the request as soon as practicable after receiving it. The Security Officer may approve or disapprove the request pending submittal of additional information by the requester. When practicable, the Security Officer's decision shall be communicated to the requester by any means at least one (1) day prior to the date of the proposed Visit, and, in all cases, the decision shall be confirmed in writing as promptly as possible.

(v) a record of all 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 Company personnel involved, shall be maintained by the Security Officer. In addition, a chronological file of all documentation associated with such Visits, together with records of approvals and disapprovals, shall be maintained for two (2) years by the Security Officer for provision at the request of the DOJ, FBI or DHS.

(vi) visitors be escorted at all times by an employee, and within conditions, including appropriate restrictions on access, set forth by the Security Officer that are commensurate with the place and purpose of the Visit.

3.3. Routine Business Visits. Notwithstanding Section 3.2, Routine Business Visits, as defined below, 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 a Domestic Communications Company; (b) do not involve the transfer or receipt of any information regarding the security of such facilities; and(c) pertain only to the commercial aspects of a Domestic Communications Company's 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 a Domestic Communications Company.

The visitation policy established under Section 3.2 may elaborate on the types of visits that qualify as Routine Business Visits.

3.4. Access by Foreign Government Authority. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, Call Associated Data, Transactional Data, or Subscriber Information stored by or on behalf of a Domestic Communications Company 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 DOJ or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Section 3.4 of this Agreement shall be reported to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to 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 described in this Section 3.4 of this Agreement.

3.5. Disclosure to Foreign Government Authorities. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide

access to:

(i) Classified, Sensitive, or Controlled Unclassified Information; or

(ii) Subscriber Information, Transactional Data, Call Associated Data, or a copy of any Wire Communications or Electronic Communication, intercepted or acquired pursuant to Lawful U.S. Process to any foreign government, identified representative, component or subdivision thereof without satisfying all applicable U.S. Federal, state and local legal requirements pertinent thereto, and obtaining the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a foreign government, or an identified representative, a component or subdivision thereof to a Domestic Communications Company for the communications, data or information identified in this Section 3.5 of this Agreement that is maintained by a Domestic Communications Company shall be referred to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. 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 described in this Section 3.5.

3.6. Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities. Within ninety (90) days after receiving legal process or requests from foreign non-governmental entities for access to or disclosure of Domestic Communications, a Domestic Communications Company shall notify the DOJ in writing of such legal process or requests, unless the disclosure of such legal process or requests would be in violation of an order of a court of competent jurisdiction within the United States.

3.7. Security of Lawful U.S. Process. Domestic Communications Companies shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified, Sensitive, and Controlled Unclassified Information in accordance with U.S. Federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information shall be under the custody and control of the Security Officer. With respect to Controlled Unclassified Information, compliance with the ITAR and the EAR shall satisfy the requirements of this Section 3.7.

3.8. Points of Contact. Within fourteen (14) days after the Effective Date, Domestic Communications Companies shall designate in writing to the FBI, DOJ and DHS, one or more nominees already holding U.S. security clearances or which the Domestic Communications Companies have a reasonable basis to believe is eligible to receive U.S.

security clearances to serve as points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process on behalf of the Domestic Communications Company. Domestic Communications Companies shall provide in writing in accordance with Section 5.13 of this Agreement, to the FBI, DOJ and DHS the name and contact information for each point of contact. The points of contact shall be assigned to the Domestic Communications Companies' security office(s) in the United States, shall be available twenty-four (24) hours per day, seven (7) days per week, and shall be responsible for accepting service and maintaining the security of Classified, Sensitive, and Controlled Unclassified Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. The points of contact shall undergo the screening process defined in Section 3.15 of this Agreement. If there is any change in the designated points of contact, Domestic Communications Companies shall notify the FBI, DOJ and DHS immediately in writing, providing updated identity and contact information. Persons serving as points of contact shall be resident U.S. citizens who hold or are eligible to receive U.S. security clearances (which may include interim security clearances), as outlined in Executive Order 12968. Domestic Communications Companies shall comply with any request by a Government Authority in the United States that a background check and/or security clearance process be completed for a designated point of contact.

3.9. Information Security Plan. Domestic Communications Companies shall develop, document, implement, and maintain an information security plan to:

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

(ii) take appropriate measures to prevent unauthorized access to data or facilities that might contain Classified, Sensitive, or Controlled Unclassified Information;

(iii) assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.12;

(iv) upon written request from the DOJ, FBI or DHS provide the name, social security number and date of birth of each person who regularly handles or deals with Sensitive Information;

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

(vi) provide that the points of contact described in Section 3.8 of this Agreement shall have sufficient authority over any of Domestic Communications Companies' employees who may handle Classified, Sensitive, or Controlled

Unclassified Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;

(vii) ensure that the disclosure of or access to Classified, Sensitive, or Controlled Unclassified Information is limited to those who have the appropriate security clearances and authority;

(viii) establish a formal incident response capability with reference to OMB Circular A-130 and NIST Special Publications 800-3, 800-18 and 800-47; and

(ix) identify the types of positions that require screening pursuant to Section 3.12, the required rigor of such screening by type of position, and the criteria by which Domestic Communications Companies will accept or reject screened persons ("Screened Personnel").

3.10. Security Officer Responsibilities and Duties. Within thirty (30) days after the Effective Date, Domestic Communications Companies shall designate, from among the points of contact selected pursuant to Section 3.8, a Security Officer within the United States with the primary responsibility for carrying out the Domestic Communications Company's obligations under Articles 2, 3 and 5 of this Agreement. The Security officer shall stand in a direct reporting relationship with the Director of Network.

3.11. Disclosure of Protected Data. In carrying out the responsibilities set forth in Section 3.10, the Security Officer shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information to any third party or to any officer, director, shareholder, employee, agent, or contractor of any Domestic Communications Company, including those who serve in a supervisory, managerial or officer role with respect to the Security Officer, unless disclosure has been approved by prior written consent obtained from the FBI, DOJ or 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. With respect to Controlled Unclassified Information, application for and receipt of an export authorization under the ITAR or the EAR, as appropriate, shall satisfy the requirements of this Section 3.11.

3.12. Screening of Personnel. Each Domestic Communications Company shall implement a thorough screening process through the Security Officer or a reputable third party to ensure that all personnel whose positions involve access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to have access to Network Management Information, Transactional Data, Call Associated Data, or Subscriber Information, persons who have access to Sensitive Information, and security personnel,

meet personnel screening requirements commensurate with the risk posed to national security by their access to facilities, equipment, or information subject to this Agreement.

(i) Domestic Communications Companies shall consult with the DOJ, FBI and DHS on the screening procedures required under this Section. The DOJ, FBI and DHS shall take into consideration Domestic Communications Companies' current and proposed screening procedures in its determination of such screening procedures, which shall be consistent with the guidance to U.S. government agencies under Executive Order 10450, and agrees to provide a list of positions subject to screening under this Section to the DOJ, FBI and DHS. The parties shall categorize the positions according to the risk posed to national security by the level of access to facilities, equipment, and information subject to this Agreement and shall agree upon the level of screening necessary to satisfy this Section for each access level. Upon request, a Domestic Communications Company shall provide to the investigation services of the DOJ, FBI and DHS, or, in the alternative, to the investigation service of the United States office of Personnel Management ("OPM"), all the information it collects in its screening process of each candidate. Candidates for these positions shall be informed, and shall consent, that the information collected during the screening process may be provided to the U.S. government. Current and newly hired personnel subject to screening will be required to sign a non-disclosure agreement approved in advance by the DOJ, FBI and DHS.

(ii) If the DOJ, FBI or DHS so desires, it may on its own, or through OPM's investigations service, conduct further background checks on screened personnel. Domestic Communications Companies will cooperate with any U.S. government agency undertaking any such further background checks.

(iii) Individuals who are rejected by a Domestic Communications Company under the screening requirements of this Section will not be hired, or, if they have begun their employment, will 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. Any rejection, pursuant to a request for further background screening under 3.12 (ii) by the DOJ, FBI, or DHS, shall be provided in writing to the Domestic Communications Company within a reasonable time, no longer than thirty (30) days after receipt of the request for further screening, in accordance with Section 5.13. Domestic Communications Companies will notify the DOJ, FBI and DHS of the transfer, departure, or job modification of any individual rejected as a result of the screening conducted pursuant to this Section within seven (7) days of such transfer or departure, and shall provide the DOJ, FBI and DHS with the name, date of birth and social security number of such individual.

(iv) 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 upon. Domestic Communications Companies shall monitor on a regular basis the status of screened personnel, and shall remove screened personnel who no longer meet the screened personnel requirements.

(v) Domestic Communications Companies shall maintain records relating to the status of screened Personnel, and shall provide these records, upon request, to the DOJ, FBI, or DHS.

3.13. Qualification and Responsibilities of Director of Network. No later than thirty (30) days after the execution of this Agreement, Domestic Communications Companies shall notify the FBI, DOJ and DHS of the identity of the Director of Network. The Director of Network shall be subject to all of the requirements of the points of contact in Section 3.8, including the screening requirements of Section 3.12 of this Agreement. The Director of Network shall have direct management oversight of the Domestic Communications Infrastructure. A Domestic Communications Company shall have the right to remove the Director of Network at any time and to appoint a replacement, subject to the terms of this Section. If the holder of the position of Director of Network changes, the Domestic Communications Company shall notify the FBI, DOJ and DHS immediately in writing, providing updated identity and contact information. In no event shall a vacancy for the position of Director of Network exist for a period of more than ninety (90) days before the Domestic Communications Company appoints a qualified candidate to fill such vacancy.

3.14. Approval of Acquisition. Acquiring or upgrading network hardware (*e.g.*, routers, switches, servers and network transmission capability) and network operating systems software requires prior approval of a Director of Network, unless subject to other procedures pursuant to a policy to be negotiated with DHS. That policy may provide for simplified procedures for non-sensitive acquisitions and upgrades (*e.g.,* vetting by the Director of Network).

3.15. Operational Control of a Domestic Communications Company Network. Except to the extent and under conditions concurred in by the FBI, DOJ and DHS in writing, operational control of the Domestic Communications Infrastructure will be restricted to Domestic Communications Company facilities located in the United States.

3.16. Notice of Obligations. Domestic Communications Companies shall instruct appropriate officials, employees, contractors, and agents as to the security restrictions and safeguards imposed by this Agreement, including the reporting requirements in Sections 5.2, 5.5, and 5.6 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.17. Access to Classified, Controlled Unclassified, or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of a U.S. government agency to deny, limit or revoke Domestic Communications Companies' access to Classified, Controlled Unclassified, and Sensitive Information under that agency's jurisdiction.

ARTICLE 4: DISPUTES

4.1. Informal Resolution. The Parties shall use their best efforts to resolve any disagreements that may arise under this 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 President of a Domestic Communications Company, the General Counsel of the FBI, and the Deputy Attorney General, Criminal Division, DOJ, and the General Counsel of DHS or their designees, unless the FBI, DOJ, or DHS believes that important national interests can be protected, or a Domestic Communications Company believes that its paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 4.2 of 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 Section 4.2 of this Agreement. If resolution of a disagreement requires access to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances for the purpose of resolving that disagreement.

4.2. Enforcement of Agreement. Subject to Section 4.1 of this 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 judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. government agency to:

(i) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty (30) days upon receiving written notice of such breach;

(ii) request that the FCC modify, condition, revoke, cancel or render null and void any license, permit, or other authorization granted or given by the FCC to any Domestic Communications Company, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against any Domestic Communications Company;

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

(iv) pursue criminal sanctions against any Domestic Communications Company,

or any director, officer, employee, representative, or agent of a Domestic Communications Company, or against any other person or entity, for violations of the criminal laws of the United States; or

(v) seek suspension or debarment of any Domestic Communications Company from eligibility for contracting with the U.S. government.

4.3. Irreparable Injury. GC and DCMG agree that the United States would suffer irreparable injury if for any reason a Domestic Communications Company failed to perform any of its material obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, GC and DCMG agree that, in seeking to enforce this Agreement against a Domestic Communications Company, the FBI, DOJ and DHS shall be entitled, in addition to any other remedy available at law or equity, to specific performance and immediate injunctive or other equitable relief.

4.4. 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.

4.5. Forum Selection. It is agreed by and among 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.

4.6. Effectiveness of Article 4. This Article 4, and the obligations imposed and rights conferred herein, shall be effective upon the execution of this Agreement by all the Parties.

ARTICLE 5: AUDITING, REPORTING, NOTICE AND LIMITS

5.1. Filings re *de jure* or *de facto* control of a Domestic Communications Company. If any Domestic Communications Company makes any filing with the FCC or any other Governmental Authority relating to the *de facto* or *de jure* control of a Domestic Communications Company except for filings with the FCC for assignments or transfers of control that are *pro forma*, the Domestic Communications Company shall promptly provide to the FBI, DOJ and DHS written notice and copies of such filing. This Section 5.1 is effective upon execution of this Agreement by all the Parties.

5.2. Control of a Domestic Communications Company. If any of the senior management of a Domestic Communications Company (including the President, Director of

Network, Chief Operating Officer, Security Officer or other senior officer) acquires any information that reasonably indicates that any single foreign entity or individual, other than DCMG has obtained or will likely obtain an ownership interest (direct or indirect) in a Domestic Communications Company 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 a Domestic Communications Company, then such member shall promptly cause to be notified the Security Officer, who in turn, shall promptly notify the DOJ, FBI and DHS in writing. Notice under this section shall, at a minimum:

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

(ii) Identify the beneficial owners of the increased or prospective increased interest in a Domestic Communications Company by the entity or individual(s) (specifying the name, addresses 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 a Domestic Communications Company.

5.3. Joint Ventures. A Domestic Communications Company 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 Company does not have *de facto* or *de jure* control over a joint venture or entity, such Domestic Communications Company 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 as a Domestic Communications Company, and (c) consult with the DOJ, FBI, or DHS about the activities of such entity. Nothing in this Section 5.3 shall be construed to relieve Domestic Communications Companies of obligations under Article 2 of this Agreement.

(ii) If a Domestic Communications Company enters into 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 Company must provide DHS with notice no later than 30 days before the joint venture offers Domestic Communications service. DHS will have 30

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

5.4. Outsourcing. If a Domestic Communications Company contracts for functions covered by this Agreement to a third party, the Domestic Communications Company shall take reasonable steps to ensure that the third party complies with the applicable terms of this Agreement with respect to functions covered by this Agreement. Such steps shall include, at a minimum:

(i) the Domestic Communications Company shall disclose this Agreement in its entirety and shall discuss with the third party those specific obligations of the Domestic Communications Company under the Agreement that relate to the contracted-for services;

(ii) the Domestic Communications Company shall promptly thereafter provide a concise report in writing, to the DHS, DOJ, and FBI setting forth, as to each such specific obligation of the Domestic Communications Company under the Agreement, the commitments on the third party that will ensure the Domestic Communications Company's compliance with each of its obligations;

(iii) the Domestic Communications Company shall notify the DHS, DOJ, and FBI no later than thirty (30) days before contracting out any function covered by this Agreement to a third Party that is identified, after reasonable inquiry by the Domestic Communications Company, as either Controlled by one or more foreign persons or combination of foreign persons under common Control, or ten (10) percent or more of whose voting equity is held, directly or indirectly, by one or more foreign persons or combination of foreign persons under common Control, which notice shall identify the name of the entity, state the functions covered by this Agreement to be performed under the contract, and include the report required under Section 5.4(ii) above. The DHS will have thirty (30) days from receipt of the notice to review and provide the Domestic Communications Company with any objection to the contract. Any objection shall be based on national security, law enforcement, or public safety grounds. If the DHS objects in accordance with this Section, the Domestic Communications Company shall not proceed with execution or performance of the contract;

(iv) the Domestic Communications Company shall include, in all contracts to perform functions covered by this Agreement with third parties that are either Controlled by, or have ten (10) Percent or more of their voting equity held,

directly or indirectly, by one or more foreign persons or combination of foreign persons under common Control, written provisions requiring the following:

(a) The third party shall execute a nondisclosure agreement in a form approved by the DOJ, FBI and DHS which will include provisions barring disclosure of information obtained pursuant to the contract to any other person without the prior written permission of the Domestic Communications Company, and holding the third Party liable for disclosure violations committed by any of its agents including directors, officers, employees, representatives or contractors;

(b) To the extent that the third party or any employee or agent of such third party has security responsibilities, or has access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to obtain Network Management Information, such persons shall be subject to personnel screening, consistent with the level of screening required under Section 3.12 of this Agreement for Domestic Communications Company personnel with similar access;

(c) To the extent that the third party or any employee or agent of such third party has access to Transactional Data, Call Associated Data or Subscriber Information, such persons shall be specifically identified to the Domestic Communications Company including each individual's name, date of birth, nationality, Passport number (if applicable), and social security number (or equivalent), and the Domestic Communications Company shall retain the right to receive and review such identifying information, to provide it to the DOJ, FBI, or DHS upon their written request, and to exclude individuals from having access to its Transactional Data, Call Associated Data or Subscriber Information;

(d) Performance of the contract may not be assigned, delegated, or transferred to any other person or entity;

(e) Such contracts shall be subject to U.S. law and the third party shall consent to the jurisdiction of the U.S. federal courts in the District of Columbia for enforcement of the contract;

(v) if the Domestic Communications Company receives information that reasonably indicates that the third party or any employee or agent has taken an action that, had it been committed by the Domestic Communications

Company, would violate an applicable provision of this Agreement, or has violated its obligations to the Domestic Communications Company related to this Agreement, the Domestic Communications Company will notify the DOJ, FBI and DHS promptly, and with consultation and, as appropriate, cooperation with the DOJ, FBI and DHS, the Domestic Communications Company will take reasonable steps necessary to rectify the situation promptly, which steps may include (among others) terminating the outsourcing arrangement with the third party, including after notice and opportunity for cure, or initiating and pursuing litigation or other remedies at law and equity; provided, however, that the Domestic Communications Company shall not contract for functions covered by this Agreement to any entity where, as a result of such contract, the entity would gain access to Sensitive Information.

Provided, however, the following types of outsourcing agreements are deemed to be routine and of a non-sensitive nature and shall be excluded from the obligations set forth in this section regarding outsourcing: (i) radio frequency ("RF") design and engineering; (ii) purchase of equipment from equipment suppliers; (iii) base station facility construction; and (iv) procurement of billing services. The Parties agree to discuss the exclusion of other classes of outsourcing contracts of a routine and non-sensitive nature.

Peering, interconnection, roaming, long distance, or other similar arrangements on which the parties may agree shall not constitute outsourced functions for purposes of this Section.

For preexisting contracts that were in force before the Effective Date, the Domestic Communications Company shall use its commercially reasonable efforts to obtain the third party's commitments to comply with all applicable undertakings set forth in this Section 5.4, and shall promptly thereafter provide to the DHS, DOJ, and FBI the report required under Section 5.4(ii) above. The applicable provisions of this Section 5.4 shall apply in full to proposed contracts that were not signed as of Effective Date, and also to preexisting contracts as they become subject to termination, renewal, or renegotiation of material terms after Effective Date.

5.5. Notice of Foreign Influence. If any member of the management of DCMG or a Domestic Communications Company (including the President, Chief Operating Officer, Director of Network, Security Officer or other senior officer) acquires any information that reasonably indicates that any foreign government, any foreign government controlled entity, or any foreign entity:

(i) plans to participate or has participated in any aspect of the day-to-day management of a Domestic Communications Company in such a way that interferes with or impedes the performance by a Domestic Communications Company of its duties and obligations under the terms of this Agreement, or interferes with or impedes the exercise by a Domestic Communications

Company of its rights under this Agreement, or

(ii) plans to exercise or has exercised, as a direct or indirect shareholder of a Domestic Communications Company, any Control of a Domestic Communications Company in such a way that interferes with or impedes the performance by a Domestic Communications Company of its duties and obligations under the terms of this Agreement, interferes with or impedes the exercise by a Domestic Communications Company of its rights under the terms of this Agreement, or in such a way that foreseeably concerns a Domestic Communications Company's obligations under this Agreement,

then such member shall promptly cause to be notified the Security Officer who in turn, shall promptly notify the FBI, DOJ and DHS in writing of the timing and the nature of the foreign government's or entity's plans and/or actions.

5.6. Reporting of Incidents. Domestic Communications Companies shall take practicable steps to ensure that, if any Domestic Communications Company officer, director, employee, contractor or agent acquires any information 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, Sensitive, or Controlled Unclassified Information, then the individual will notify the Security Officer, who will in turn notify the FBI and the DOJ in the same manner as specified in Section 5.5. This report shall be made no later than ten (10) calendar days after the Domestic Communications Company acquires information indicating a matter described in this Section 5.6(a)-(d) of this Agreement. The Domestic Communications Company shall lawfully cooperate in investigating the matters described in this section of this Agreement. The Domestic Communications Company need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

5.7. Non-Retaliation. Each Domestic Communications Company shall, by duly authorized action of its President, ratified by its Board of Directors, adopt and distribute an official corporate policy that strictly prohibits a Domestic Communications Company 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 5.2, 5.5 or 5.6 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 FBI, DOJ and DHS by the Security Officer under Sections 5.2, 5.5 or 5.6 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 a Domestic Communications Company of any material term of such corporate policy shall constitute a breach of this Agreement.

5.8. Third Party Audits. Domestic Communications Companies shall retain and pay for a neutral third party to conduct audits objectively on an annual basis to assess its compliance with the terms of this Agreement, and shall furnish to the DOJ, FBI and DHS a report in accordance with Section 5.11. Domestic Communications Companies shall provide notice of its selected auditor to the DOJ, FBI and DHS, and the DOJ, FBI and DHS shall be able to review and approve or disapprove the selected auditor within thirty (30) days of receiving notice. Domestic Communications Companies shall provide DOJ, FBI and DHS with a description of the scope and purpose of the audits at least three (3) months in advance of commencing an audit, and DOJ, FBI and DHS shall have the right to review and approve the terms defining the scope and purpose of the audits. Domestic Communications Companies shall ensure that the auditor has full and unimpeded corporate authority to conduct the audits without restriction or limitation by any officer, director, employee, contractor or agent of the Domestic Communications Company. The terms defining the scope and purposes of the audits shall include, at a minimum, authority for the auditor (a) to review and analyze the Domestic Communications Company's policies and procedures designed to implement this Agreement, all relevant information related to the configuration of the Domestic Communications Company's network, all minutes of meetings held or actions taken by the Domestic Communications Company's Board of Directors or Committees of the Board in accordance with this Agreement, an Security officer logs and records including records related to facility visits, personnel screening data, and any reports submitted in accordance with Section 5.9 of this Agreement; and (b) to conduct a reasonable number of unannounced inspections of the Domestic Communications Company's facilities each year, a reasonable volume of random testing of network firewalls, access points and other systems for potential vulnerabilities, and a reasonable number of confidential interviews of the Domestic Communications Company's officers, directors, employees, contractors or agents concerning compliance with this Agreement. Upon request, the Domestic Communications Company shall provide the DOJ, FBI or DHS with access to facilities, information, and personnel consistent with Sections 5.10 and 5.11 below in the event that the DOJ, FBI and DHS wishes to conduct its own annual audit of the Domestic Communications Company's compliance with this Agreement.

5.9. Access to Information and Facilities. FBI, DOJ and DHS may visit with reasonable advance notice any part of a Domestic Communications Company's 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 the FBI, DOJ, or DHS to verify compliance with the then-effective terms of this Agreement.

5.10. Access to Personnel. Upon reasonable notice from the FBI, DOJ, or DHS,

Domestic Communications Companies will make available for interview officers or employees of Domestic Communications Companies, and will require contractors to make available appropriate personnel located in the United States who are in a position to provide information to verify compliance with the terms of this Agreement; provided that the Parties shall, in good faith, take into consideration the actual availability of the necessary individuals.

5.11. Annual Report. On or before the last day of January of each year after the Effective Date, the Chief Executive Officer, President or other designated senior corporate officer of the Domestic Communications Companies shall submit to the FBI, DOJ and DHS a report assessing the Domestic Communications Companies compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

(i) a copy of Security audit reports compiled by the third party auditor conducted pursuant to Section 5.8 of this Agreement;

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

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

(iv) 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

(v) identification of any other issues that, to the Domestic Communications Company's knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement.

All 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.

5.12. Information and Reports Concerning Network Architecture. If requested by the DOJ, FBI and DHS, Domestic Communications Company shall provide to the DOJ, FBI and DHS, 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 operations 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 Company's IP 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 Company as well as of the Domestic Communications Company's operating and administrative software.

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

Once a report has been made under this Section 5.12, the Domestic Communications Company 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" 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.

5.13. Notices. Effective upon execution of this Agreement by all the Parties, 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 (a) delivered personally, or (b) sent by facsimile, or (except as noted below) (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 others addresses as the Parties may designate in accordance with this Section:

Department of Justice
Assistant Attorney General
Criminal Division

Main Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530
Federal Bureau of Investigation
General Counsel
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Department of Homeland Security
Washington, D.C. 20528
Attn: General Counsel, Office of the General Counsel
Telephone: 202-692-4237
Fax: 202-282-8415
(By Personal Delivery or E-mail Only)

Federal Bureau of Investigation
The Assistant Director
National Security Division
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Guam Cellular and Paging, Inc.
Attn: President
Century Plaza
219 South Marine Drive, Suite 206
Tamining, Guam 96913
Telephone: 671-688-6400
Fax: 671-649-7247

DoCoMo Guam Holdings, Inc.
Attn: President
c/o NTT DoCoMo USA, Inc.
1399 New York Ave., NW Suite 450
Washington, D.C. 20005.
Telephone: 202-639-9377
Fax: 202-639-9588

ARTICLE 6: FREEDOM OF INFORMATION ACT

6.1. Protection from Disclosure. The DOJ, FBI and DHS shall take all reasonable measures to protect from public disclosure all information submitted by a Domestic Communications Company in accordance with the terms of this Agreement to the DOJ, FBI or DHS in connection with this Agreement and clearly marked with the legend "Confidential; subject to protection under 5 U.S.C. § 552(b); not to be released without

notice to the Domestic Communications Company" or similar designation. Such markings shall signify that it is the Domestic Communications Company's position that the information so marked constitutes "trade secrets" and/or "commercial or financial information obtained from a person and privileged or confidential," or otherwise warrants protection within the meaning of 5 U.S.C. § 552(b)(4). For the purposes of 5 U.S.C. § 552(b)(4), the Parties agree that information so marked is voluntarily submitted. If a request is made under 5 U.S.C. § 552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, the DOJ, FBI or DHS, as appropriate, shall notify the Domestic Communications Company of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 1987). If the Domestic Communications Company objects to the intended disclosure and its objections are not sustained, the DOJ, FBI, or DHS, as appropriate, shall notify the company of its intention to release (as provided by Section 5 of Executive Order 12600) not later than five business days prior to disclosure of the challenged information. The Parties note that information submitted by a Domestic Communications Company in accordance with the terms of this Agreement may be protected from disclosure under the Critical Information Infrastructure Act of 2002.

6.2. Use of Information for U.S. Government Purposes. Nothing in this Agreement shall prevent the FBI, DOJ or DHS from lawfully disseminating information as appropriate to seek enforcement of this Agreement, or from lawfully sharing information as appropriate with other Federal, state, or local government agencies to protect public safety, law enforcement, or national security interests, provided that the FBI, DOJ or DHS take all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

6.3. Unlawful Disclosure of Information. The DOJ, FBI and DHS acknowledge that officers and employees of the United States and of any department or agency thereof are subject to liability under 18 U.S.C. § 1905 for unlawful disclosure of information provided to them by other Parties to this Agreement.

ARTICLE 7: FCC CONDITION

7.1. FCC Approval. Upon the execution of this Agreement by all the Parties, the DOJ, FBI and DHS shall promptly 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.), the DOJ, FBI and DHS have no objection to the FCC's grant of the applications filed with the FCC in FCC IB Docket No. 06-96. This Section 7.1 is effective upon execution of this Agreement by all the Parties.

7.2. Future Applications. DCMG agrees that, in any application or petition by any Domestic Communications Company to the FCC for licensing or other authority filed with or granted by the FCC after the Effective Date, except with respect to *pro forma* assignments or *pro forma* transfers of control, the Domestic Communications Company shall request that

the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 8.9, the FBI, DOJ and DHS reserve the right to object, formally or informally, to the grant of any other FCC application or petition of a Domestic Communications Company for a license or other authorization under Titles II or 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 their ability to enforce the laws, preserve the national security, and protect the public safety raised by the transactions underlying such applications or petitions.

ARTICLE 8: OTHER

8.1. Right to Make and Perform Agreement. DCMG and GC each represent that each 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 DCMG and GC enforceable in accordance with its terms.

8.2. 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.

8.3. 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 DCMG or GC, (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 (including without limitation authority pursuant to International Emergency Economic Powers Act) over the activities of DCMG or GC. Nothing in this Agreement is intended to or is to be interpreted to require the Parties to violate any applicable U.S. law.

8.4. Statutory References. All references in this Agreement to statutory provisions shall include any future amendments to such statutory provisions.

8.5. Non-Parties. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties and any Governmental Authorities entitled to effect Electronic Surveillance pursuant to Lawful U.S. Process.

8.6. Modifications. This Agreement may only be modified by written agreement signed by all of the Parties. The DOJ, FBI and DHS agree to consider in good faith and promptly possible modifications to this Agreement if DCMG or GC believes that the obligations imposed on DCMG or GC 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) days after approval in writing by the Parties.

8.7. Changes in Circumstances for DCMG or a Domestic Communications Company. The DOJ, FBI and DHS agree to negotiate in good faith and promptly with respect to any request by DCMG or a Domestic Communications Company for relief from application of specific provisions of this agreement: (a) if the Domestic Communications Company provides 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 DCMG's, or the Domestic Communications Company's competitive position.

8.8. Changes in Circumstances for the DOJ, FBI or DHS. If, after the date that all the Parties have executed this Agreement, the DOJ, FBI or DHS finds that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns presented, then the other Parties 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, enforce the laws or protect the safety of the public, the parties will work promptly to amend the agreement to implement such advances.

8.9. 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.

8.10. 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.

8.11. Successors and Assigns. This Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns.

8.12. 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.

8.13. Termination of Agreement. If the SPA and APA is terminated prior to the Effective Date, DCMG or GC shall promptly provide written notification of such termination to the FBI, DOJ and DHS, and upon receipt of such written notice, this Agreement shall automatically terminate. After the Effective Date, this Agreement shall terminate upon thirty (30) days prior written notice from DCMG or GC to the FBI, DOJ and DHS.

8.14 Suspension of Agreement With Respect to a Domestic Communications Company. This Agreement shall be suspended upon thirty (30) days notice to the DOJ, FBI and DHS with respect to any covered Domestic Communications Company entity if said entity is no longer a Domestic Communications Company.

8.15. Suspension of Agreement If No Significant Foreign Ownership. This Agreement shall be suspended in its entirety with respect to DCMG and all Domestic Communications Companies thirty (30) days after receipt from DCMG or a Domestic Communications Company of notice and documentation reasonably satisfactory to the DOJ, FBI and DHS that neither DCMG nor any other foreign entity either Controls a Domestic Communications Company or holds, directly or indirectly, a ten (10) percent or greater interest in a Domestic Communications Company, unless the DOJ, FBI and DHS notify a Domestic Communications Company within said thirty (30) day period that this Agreement shall not be suspended in order to protect U.S. national security, law enforcement, and public safety concerns. If this Agreement is not suspended pursuant to this provision, the DOJ, FBI and DHS agree to consider promptly and in good faith possible modifications to this Agreement. Notwithstanding anything to the contrary in this Section 8.15, this Agreement shall remain in effect with respect to DCMG and the Domestic Communications Companies for so long as (and the obligations of DCMG and the Domestic Communications Companies shall not be suspended and any suspension of the obligations of GC shall terminate if) DCMG or any other foreign entity shall either Control or hold, at any time does hold, or is a party to an agreement to hold, directly or indirectly, a ten (10) percent or greater ownership interest, as determined in accordance with 47 C.F.R. § 63.09, in any Domestic Communications Company or any transferee or assignee of the FCC licenses or authorizations held by a Domestic Communications Company.

8.16. Pledging of Stock or Assets of a Domestic Communications Company. Nothing in this Agreement shall be interpreted to prevent DCMG from pledging assets of any Domestic Communications Company in connection with the borrowing of funds and similar financial activities by a Domestic Communications Company, nor shall such pledging of stock or assets excuse performance of the obligations in this Agreement by a Domestic Communications Company.

8.17. Effectiveness of Article 8. This Article 8, and the obligations imposed and rights conferred herein, shall be effective upon the execution of this Agreement by all the Parties.
This Agreement is executed on behalf of the Parties:
This Agreement is executed on behalf of the Parties:

Guam Cellular and Paging, Inc.

Date: _____

By: _____
Printed Name:
Title:

DoCoMo Guam Holdings, Inc.

suspended in order to protect U.S. national security, law enforcement, and public safety concerns. If this Agreement is not suspended pursuant to this provision, the DOJ, FBI and DHS agree to consider promptly and in good faith possible modifications to this Agreement. Notwithstanding anything to the contrary in this Section 8.15, this Agreement shall remain in effect with respect to DCMG and the Domestic Communications Companies for so long as (and the obligations of DCMG and the Domestic Communications Companies shall not be suspended and any suspension of the obligations of GC shall terminate if) DCMG or any other foreign entity shall either Control or hold, at any time does hold, or is a party to an agreement to hold, directly or indirectly, a ten (10) percent or greater ownership interest, as determined in accordance with 47 C.F.R. § 63.09, in any Domestic Communications Company or any transferee or assignee of the FCC licenses or authorizations held by a Domestic Communications Company.

8.16. Pledging of Stock or Assets of a Domestic Communications Company. Nothing in this Agreement shall be interpreted to prevent DCMG from pledging assets of any Domestic Communications Company in connection with the borrowing of funds and similar financial activities by a Domestic Communications Company, nor shall such pledging of stock or assets excuse performance of the obligations in this Agreement by a Domestic Communications Company.

8.17. Effectiveness of Article 8. This Article 8, and the obligations imposed and rights conferred herein, shall be effective upon the execution of this Agreement by all the Parties.
This Agreement is executed on behalf of the Parties:
This Agreement is executed on behalf of the Parties:

Guam Cellular and Paging, Inc.

Date: _____

By: _____
Printed Name:
Title:

DoCoMo Guam Holdings, Inc.

Date: 10/4/06

By: [signature]
Printed Name: Elaine N. Lammert
Title: Deputy General Counsel

Federal Bureau of Investigation

Date: _____

By: _____
Printed Name:
Title:

Federal Bureau of Investigation

Date: 10/10/06

By: _____
Printed Name: Sigal P. Mandelker
Title: Deputy Assistant Attorney General

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

United States Department of Homeland Security

Date: 10/13/06

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

EXHIBIT A

CONDITION TO FCC AUTHORIZATION IT IS FURTHER ORDERED, that consent to the assignment, transfer of control, and declaratory ruling pursuant to 47 U.S.C. § 310(b)(4) are subject to compliance with the provisions of the Agreement attached hereto among DCMG and GC on the one hand, and the United States Department of Justice ("DOJ"), the Federal Bureau of Investigation ("FBI"), and the United States Department of Homeland Security ("DHS"), on the other, dated 10/06, which Agreement is designed to address national security, law enforcement, and public safety issues of the DOJ, the FBI and the DHS regarding the authority granted herein. Nothing in this 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.

This Agreement is executed on behalf of the Parties:

Guam Cellular and Paging, Inc.

Date: _____

By: _____
Printed Name:
Title:

DoCoMo Guam Holdings, Inc.

Date: _____

By: _____
Printed Name: TOSHINARI KUNIEDA
Title: Chairman

Federal Bureau of Investigation

Date: _____

By: _____
Printed Name:
Title:

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

United States Department of Homeland Security

Date: _____

By: _____
Printed Name:
Title:

This Agreement is executed on behalf of the Parties:

Guam Cellular and Paging, Inc.

Date: _____

By: _____
Printed Name: Mark Chamberlin
Title: President

DoCoMo Guam Holdings, Inc.

Date: _____

By: _____
Printed Name:
Title:

Federal Bureau of Investigation

Date: _____

By: _____
Printed Name:
Title:

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

United States Department of Homeland Security

Date: _____

By: _____
Printed Name:
Title: