

## AGREEMENT

**THIS AGREEMENT** (the “Agreement”) is made as of the date of the last signature affixed hereto, by and between Level 3 Communications, Inc. (“Level 3 Parent”), including its subsidiaries and affiliates (collectively with Level 3 Parent, “Level 3”) 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,” with DOJ and DHS, “Government Parties”) on the other (each referred to individually as a “Party” and collectively as the “Parties”).

## RECITALS

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

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

**WHEREAS**, it is critical to the well-being of the Nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (see *e.g.*, Executive Order 13231, Critical Infrastructure Protection in the Information Age, and Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection);

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

**WHEREAS**, Level 3, through one or more subsidiaries, offers transport, high-speed Internet protocol (“IP”), virtual private network, dark fiber, managed modem, collocation, media and content delivery, and voice services over its terrestrial intercity, metropolitan fiber, and transoceanic network facilities;

**WHEREAS**, Global Crossing Limited (“GCL”), through one or more of its subsidiaries, offers transport and infrastructure, switched data, voice, collaboration and conferencing, data center and hosting, and media transport services over its terrestrial and transoceanic network facilities;

**WHEREAS**, Level 3 Parent will acquire GCL pursuant to an Agreement and Plan of Amalgamation dated April 10, 2011, which provides that GCL will be renamed Level 3 GC Limited and will be a wholly-owned, direct subsidiary of Level 3 upon consummation of the acquisition.

**WHEREAS**, Level 3 Parent’s acquisition of GCL will return GCL to U.S. management control and predominantly U.S. ownership and replace the majority interest of STT Crossing Ltd (“STT Crossing”) in GCL with a minority interest initially of approximately 23.92 percent in Level 3 Parent as of the closing of the transaction (and not to exceed 34.5 percent thereafter, absent written consent by a majority of Level 3 Parent’s directors, excluding directors designated by STT Crossing) and, as of the closing of the transaction, the right to designate three (3) directors for appointment to Level 3 Parent’s eleven (11)-member Board of Directors, with STT Crossing participating in Level 3 Parent only at the shareholder and Board of Directors levels;

**WHEREAS**, Level 3 and GCL and its subsidiaries have filed applications seeking the consent of the Federal Communications Commission (“FCC”) to transfer control of the GCL subsidiaries’ cable landing licenses, domestic and international Section 214 authority, and satellite earth station authorizations to Level 3 (the “Applications”);

**WHEREAS**, Level 3 has filed with the FCC a petition for declaratory ruling finding that aggregate indirect foreign ownership in Level 3 subsidiaries holding common-carrier radio licenses in excess of the limitation in 47 U.S.C. § 310(b)(4) would serve the public interest (the “Petition”);

**WHEREAS**, certain subsidiaries of Level 3 and GCL have and will continue to have direct physical and electronic access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

**WHEREAS**, certain subsidiaries of Level 3 and GCL have and will continue to have an obligation to protect from unauthorized disclosure the contents of wire and electronic communications to and from the United States under U.S. law; and

**WHEREAS**, the Government Parties will request that the FCC’s grant of the transfer-of-control applications filed by Level 3 and GCL and its subsidiaries be made subject to resolution of issues relating to national security, law enforcement, and public safety, and whereas Level 3 has agreed to enter into this Agreement with the Government Parties to address issues raised by the Government Parties and to jointly petition that the FCC condition the requested authorization on compliance with this Agreement;

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

## **ARTICLE 1: DEFINITION OF TERMS**

As used in this Agreement:

1.1 “**Access**” or “**Accessible**” means the ability to physically or logically undertake any of the following actions: (a) read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system or a network; (b) add, edit or alter information or technology stored on or by software, hardware, a system or a network; and (c) alter the physical or logical state of software, hardware, a system or a network (*e.g.*, turning it on or off, changing configuration, removing or adding components or connections).

1.2 “**Affiliate**” means any entity that Level 3 Controls, as defined in Section 1.5 of this Agreement.

1.3 “**Cable System**” means all equipment, facilities, and services pertaining to the Yellow, Atlantic Crossing-1, Atlantic Crossing-2, Mid-Atlantic Crossing, Pan American Crossing, or South American Crossing system, and any other undersea cable system owned or Controlled, presently or in the future, by Level 3 and which land in the United States; and all associated network operations centers. “Cable System” does not include an undersea cable system in which Level 3 may have a fractional, non-controlling ownership interest.

1.4 “**Classified Information**” shall have the meaning indicated in Executive Order 12958, as amended by Executive Order 13292, or any successor executive order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act of 1954, to require protection against unauthorized disclosure.

1.5 “**Control**” and “**Controls**” means the power, direct or indirect, whether or not exercised, and whether or not exercised or exercisable through the ownership of a majority or a dominant minority of the total outstanding voting securities of an entity, or by proxy voting, contractual arrangements, or other means, to determine, direct, or decide matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding:

- a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;
- b) the dissolution of the entity;
- c) the closing and/or relocation of the production or research and development facilities of the entity;
- d) the termination or nonfulfillment of contracts of the entity;
- e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.5(a) through (d); or
- f) Level 3’s obligations under this Agreement.

1.6 “**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.

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

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

1.9 **“Domestic Communications Infrastructure”** means: (i) transmission, switching, bridging, routing equipment (including software and upgrades), servers, security appliances, and fiber and copper cable and associated facilities owned (to include leased) and controlled by or on behalf of Level 3 to provide, process, direct, control, supervise, or manage Domestic Communications; (ii) facilities and equipment owned (to include leased) and controlled by or on behalf of Level 3 to provide Domestic Communications services and which are physically located in the United States; and (iii) facilities owned (to include leased) and controlled by or on behalf of Level 3 or to control the equipment described in (i) and (ii) above. Excluded equipment and facilities include those controlled by service providers other than Level 3 that are:

- (1) Interconnection and collocation communications providers, including customers collocating such equipment in the collocation space of Level 3 or cross-connecting to other parties in the “meet me” space of Level 3; however, main distribution frames, fiber, interconnection gateways in interconnection and collocation facilities and operated by Level 3, and any other equipment, which has the ability to exert command or control influence over the facilities and equipment set forth in subsections (i), (ii), and (iii) above, would not be excluded; or
- (2) Providers of services or content that are:
  - (a) Accessible using the communications services of Level 3; and
  - (b) Available in substantially similar form and on commercially reasonable terms through communications services of companies other than Level 3.

The phrase “on behalf of,” as used in this part, does not include entities with which Level 3 has contracted for peering, interconnection, roaming, long distance, or other similar arrangements.

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.

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

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

1.12 **“Electronic Surveillance,”** for the purposes of this Agreement, includes: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2),

(4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (d) acquisition of location-related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) Access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

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

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

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

1.16 “**Lawful U.S. Process**” means lawful U.S. federal, state, or local Electronic Surveillance or other court orders, processes, or authorizations issued by or on behalf of U.S. federal, state, or local government agencies for physical search or seizure, production of tangible things, or Access to or disclosure of Domestic Communications, Transactional Data, or Subscriber Information.

1.17 “**Management**” means the officers and members of the Boards of Directors of Level 3.

1.18 “**Network Management Information**” means network management operations plans, processes and procedures; descriptions of the placement of network operations centers and linkages (for service offload or administrative activities) to other domestic and international carriers, Internet service providers, and other critical infrastructures; descriptions of networks and operations processes and procedures for management control and relation to the backbone infrastructure(s); description of any unique or proprietary control mechanisms as well as operating and administrative software; network performance information; network access ability and procedures; data generated from network monitoring, analysis, and provisioning tools; and network configurations, security and firewall configurations.

1.19 “**Network Operations Center**” or “**NOC**” means the locations and facilities designated as such by Level 3 for purposes of performing network management, monitoring, maintenance, or other operational functions for Domestic Communications Infrastructure or the U.S.-territory portion of a Cable System.

1.20 “**Offshore**” or “**Offshoring**” means performing obligations of this Agreement that are normally performed within the territorial limits of the United States, through the use of personnel

outside the territorial limits of the United States, whether those personnel are employees of Level 3 or third-parties.

1.21 **“Outsource” or “Outsourcing”** means performing obligations of this Agreement which are normally performed by personnel of Level 3 through the use of contractors.

1.22 **“Principal Equipment”** means the primary electronic components of a submarine cable system, to include the hardware used at the NOC(s), landing station(s) and the cable itself, such as servers, repeaters, submarine line terminal equipment (SLTE), system supervisory equipment (SSE), power feed equipment (PFE), tilt and shape equalizer units (TEQ/SEQ), optical distribution frames (ODF), and synchronous optical network (SONET), synchronous digital hierarchy (SDH), wave division multiplexing (WDM), dense wave division multiplexing (DWDM), coarse wave division multiplexing (CWDM) or optical carrier network (OCx) equipment, as applicable.

1.23 **“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 Sections 1.767, 25.119, 63.24 of the FCC’s Rules (47 C.F.R. §§ 1.767, 25.119, 63.24).

1.24 **“Security Officer”** means the Person designated pursuant to Section 3.7 of this Agreement.

1.25 **“Sensitive Information”** means information that is not Classified Information regarding: (a) the persons or facilities that are the subjects of Lawful U.S. Process; (b) the identity of the Government Authority or Government Authorities serving such Lawful U.S. Process; (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance; (d) the means of carrying out Electronic Surveillance; (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, (g) 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, and (h) other information that is not Classified Information but is designated in writing by an authorized official of a federal, state, or local law enforcement agency or a U.S. intelligence agency as “Sensitive Information” of some type recognized by the agency involved. The designation “Sensitive” as used in this Section includes but is not limited to information marked or labeled “Official Use Only,” “Limited Official Use Only,” “Law Enforcement Sensitive,” “Sensitive Security Information,” “Sensitive but Unclassified,” “Controlled Unclassified Information,” “Protected Critical Infrastructure Information,” or other similar designations.

1.26 **“Subscriber Information”** means all records or other information relating to customers or subscribers of Level 3 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.

1.27 “**Technical Compliance Officer**” means the Person designated pursuant to Section 3.7 of this Agreement.

1.28 “**Transactional Data**” includes the following when associated with a Domestic Communication but does not include the content of any communication: (a) “call identifying information,” as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator; (b) any information related to the sender or recipient of that Domestic Communication, including, without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post-cut-through dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold; (c) any information relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, IP addresses, Uniform Resource Locators (“URLs”), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (e) below; (d) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control (“MAC”) or IP addresses (including source and destination), URL’s, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics, including electronic mail headers showing From: and To: addresses; and (e) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.

1.29 “**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.

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

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

## **ARTICLE 2: OPERATIONS, FACILITIES, INFORMATION STORAGE AND ACCESS**

2.1 **Operational Requirements.** With respect to the operation of Domestic Communications Infrastructure and Cable Systems, Level 3 agrees as follows:

- (a) Except as provided in Section 2.1(b) below, all Domestic Communications Infrastructure of Level 3 shall at all times be located in the United States and shall be controlled, directed, supervised, and managed by Level 3.
- (b) The primary U.S. NOCs for any Domestic Communications Infrastructure shall be maintained and remain within the United States and U.S. territories, to be operated by Level 3, exclusively using Screened Personnel (as defined in Section 3.11). Level 3 may nonetheless use the United Kingdom NOC for routine day-to-day management of any of the Cable Systems as such management is in existence as of the Effective Date.
- (c) All Domestic Communications that are carried through, in whole or in part, the Domestic Communications Infrastructure shall pass through a facility under the control of Level 3 and be physically located in the United States from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. Level 3 will provide technical or other assistance to facilitate such Electronic Surveillance.
- (d) With respect to the Cable Systems, Level 3 shall have the ability to promptly and effectively interrupt in whole or in part traffic to and from the United States on each Cable System by disabling or disconnecting circuits at the U.S. cable landing or at other locations within the United States.
- (e) With respect to the Cable Systems, Level 3 shall have the ability to isolate any U.S. NOC, U.S. landing station, or the connecting cable segment from the rest of the Cable System.
- (f) Within sixty **(60) calendar days** after the date of consummation of Level 3's acquisition of GCL, each Cable System shall be configured so that a U.S. NOC will be able to view the status of the Cable System and individual cable segments and override the United Kingdom NOC as necessary.

**2.2 Compliance with Lawful U.S. Process.** Level 3 shall configure the Domestic Communications Infrastructure to be capable of complying, and the employees of Level 3 in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

- (a) Lawful U.S. Process;
- (b) 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 Level 3 that is enumerated in this Agreement;
- (c) The orders of the President of the United States in the exercise of his/her authority under the Cable Landing License Act of 1921, as amended (47 U.S.C. §§ 34-39)



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

- (d) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

**2.3 Cable System Infrastructure.** Within **ten (10) business days** after the Effective Date, Level 3 shall provide to the Government Parties updated lists of:

- (a) the Principal Equipment used in all the Cable Systems, to include information on the Principal Equipment’s manufacturer and model; and
- (b) all contracts held by Level 3 for the maintenance and security of the Cable Systems (the “Cable Systems Contract List”).

Level 3 shall provide at least **fifteen (15) business days’** advance written notice to the Government Parties prior to performing any maintenance, repair, or replacement that would result in any material modification to the Principal Equipment list for any Cable System. Level 3 need not comply with the advance notice requirement for any maintenance, repair or replacement that is undertaken in response to an unforeseen or uncontrollable event and is necessary to ensure the continued operability of any Cable System; however, in such circumstances Level 3 shall provide advance notice of the modification to the Government Parties if practicable, and if impracticable, within five **(5) business days** after the material modification of the Principal Equipment. Level 3 shall provide at least **thirty (30) business days’** advance written notice to the Government Parties prior to making any material modifications to its contracts for Cable System maintenance and security. Level 3 agrees to make the Cable System-related Network Management Information available to the Government Parties upon request. Level 3 shall negotiate in good faith to resolve any national security, law enforcement, or public safety concerns the Government Parties may raise with respect to each Cable System’s Principal Equipment, contracts, and Network Management Information.

**2.4 Network and Telecommunications Architecture.** Within **sixty (60) days** of the Effective Date, Level 3 shall provide to the Government Parties a comprehensive description of its Domestic Communications Infrastructure network and telecommunications architecture. This description shall include locations of all principal equipment, including core routers, servers, switches, operational systems software, and network security applications and software, as well as architecture interconnect diagrams, architecture flow diagrams, and architecture context diagrams. This comprehensive description shall include the following information regarding the interconnections and control of the Domestic Communications Infrastructure:

- (a) 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;

- (b) a description of the placement of NOCs, data centers, and Operations Support System (OSS) hosting centers,
- (c) a description of Level 3's IP networks and operation processes, procedures for management control, and its operational processes and procedures for interconnection control and peering relationships with the backbone infrastructures of other service providers;
- (d) a report of Network Management Information that includes an assurance that network performance satisfies FCC rules and reporting requirements; and
- (e) a description of any unique or proprietary control mechanisms of Level 3 as well as of Level 3's operating and administrative software.

2.5 **Information Storage and Access.** Unless otherwise agreed to by the Parties, in writing, Level 3 shall store in the United States a primary copy of the information listed below. A primary copy is a trusted master copy stored in a document, file and/or database repository controlled and/or managed by Level 3 and used for data analysis and/or verification. This section shall apply to:

- (a) stored Domestic Communications;
- (b) 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 domestic customer or subscriber of Level 3, if such communications are stored by or on behalf of Level 3 for any reason;
- (c) Transactional Data, if such data are stored by or on behalf of Level 3 for any reason;
- (d) Subscriber Information, if such information is stored by or on behalf of Level 3 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; and
- (e) 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. Such records shall be stored for at least **twenty-four (24) months** for customers or subscribers that are domiciled in the U.S;
- (f) Network Management Information; and

- (g) access logs pertaining to Domestic Communications Infrastructure. Such logs shall be stored for at least eighteen (18) months.

The phrase “on behalf of” as used in this Section does not include entities with which Level 3 has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree. Level 3 may provide controlled remote access to information listed in paragraphs (c), (d), (e), and (f) above to Outsourced or Offshored personnel screened pursuant to Level 3’s Outsourcing and Offshoring control and access policy referenced in Section 3.14 of this Agreement; however, such controlled remote access shall not include the ability to alter or delete the information listed in paragraphs (c), (d), (e), (f), CPNI, or personal identifier information other than within the constraints of Level 3’s Outsourcing and Offshoring control and access policies, referenced in Section 3.14.

Level 3 shall in no case Outsource or Offshore functions involving Access to Classified Information, Sensitive Information, or Lawful U.S. Process.

**2.6 Storage Pursuant to 18 U.S.C. § 2703(f).** Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Government Authority within the United States to preserve any information in the possession, custody, or control of Level 3, including any information that is listed in Section 2.5 above, Level 3 shall store such information in the United States.

**2.7 Compliance with U.S. Law.** Nothing in this Agreement shall excuse Level 3 from any obligation they may have to comply with U.S. legal requirements for the retention, preservation, or production of information, records or data as well as all applicable requirements of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, *et seq.*

**2.8 Storage of Classified Information.** The storage of Classified and Sensitive Information by Level 3 outside 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 or approved by a U.S. government organization.

**2.9 CPNI.** Level 3 shall comply, with respect to Domestic Communications, with all applicable FCC rules and regulations governing access to and storage of CPNI.

### **ARTICLE 3: SECURITY**

**3.1 Measures to Prevent Improper Use or Access.** Level 3 shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to Access, obtain, or disclose Domestic Communications, Transactional Data, Subscriber Information, Classified Information, or Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. Level 3 shall submit the policies and procedures regarding these measures to the Government Parties for review within **sixty (60) days** of the Effective Date of this Agreement. Level 3 agrees to meet and confer with the Government Parties and reasonably address any concerns the Government Parties may raise about the policies or the procedures described therein.

**3.2 Access or Disclosure Requests.** Level 3 shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, Transactional Data, or Subscriber Information stored by Level 3 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 3.2 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. Level 3 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 3.2 of this Agreement.

**3.3 Access or Disclosure Requests from Foreign Government Authorities.** Level 3 shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

- (a) Classified or Sensitive Information; or
- (b) Subscriber Information or Transactional Data, including 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, an identified representative, a component or subdivision thereof to Level 3 for the communications, data or information identified in this Section 3.3 of this Agreement that is maintained by Level 3 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 by and known to the Security Officer 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. Level 3 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 3.3.

**3.4 Access or Disclosure Requests from Foreign Non-Governmental Entities.** Within **ninety (90) days** of receipt, Level 3 shall notify DOJ in writing of legal process or requests by foreign nongovernmental entities to Level 3 for access to or disclosure of Domestic Communications 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.

**3.5 Security of Lawful U.S. Process.** Level 3 shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified and Sensitive Information in accordance with U.S. federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process and Classified and Sensitive Information shall be under the custody and control of the Security Officer.

3.6 **Points of Contact.** Level 3 has previously designated and maintained a Point of Contact with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to its customers or subscribers. Within **thirty (30) days** of the Effective Date of this Agreement, Level 3 shall designate in writing at least two Points of Contact assigned to Level 3's offices in the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The Points of Contact shall be available **twenty-four (24) hours** per day, **seven (7) days** per week and shall be responsible for accepting service and maintaining the security of Classified Information, Sensitive Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. Level 3 shall notify the Government Parties of all future changes in the designated Points of Contact, or the designation of alternate Points of Contact, in **ten (10) business days** or fewer. The Points of Contact shall be resident U.S. citizens who are eligible for appropriate U.S. security clearances, and shall serve as Points of Contact for Level 3 unless and until the Government Parties are notified of any change in designation. Level 3 shall cooperate with any request by a Government Authority within the United States that a background check, security clearance process or both be completed for a Point of Contact.

3.7 **Designation of Security Officer and Technical Compliance Officer.** Within **thirty (30) days** of the Effective Date, Level 3 shall designate a Security Officer. The Security Officer shall have the appropriate senior-level corporate authority within Level 3, and the necessary resources and skills, to enforce this Agreement, implement the access or disclosure request requirements, information security plan, the personnel screening process requirements, and the visitation policy in Sections 3.2, 3.3, 3.9, 3.11, 3.12, and 3.13 of this Agreement, and to act as liaison to the Government Parties regarding compliance with this Agreement and any national security issues. The Security Officer shall have access to the business information of Level 3 necessary to perform his or her duties. Level 3 shall consult in advance of the initial designation of the Security Officer with the Government Parties regarding the selection and identify of the Security Officer and shall reasonably address any concerns raised by the Government Parties regarding the selection and identity of the Security Officer.

Within **thirty (30) days** of the Effective Date, Level 3 shall also employ a Technical Compliance Officer (TCO) who will have the appropriate authority and skills to implement, in consultation with the Security Officer, the terms of this Agreement and to address security concerns identified by the Government Parties.

The Security Officer and the TCO shall both:

- (a) Be a resident U.S. citizen who possesses U.S. citizenship only (i.e., may not be dual-nationals);
- (b) If not already in possession of U.S. security clearances, shall be eligible, at the sole discretion of the Government Parties, to hold such security clearances immediately upon appointment;

- (c) Be subject to the screening process described in Sections 3.11 and 3.12; and
- (d) In the case of the Security Officer, be a corporate officer with appropriate authority, skills, and resources to enforce this Agreement with respect to Level 3.

Within **thirty (30) days** of the Effective Date, Level 3 shall notify the Government Parties of the individuals initially selected for each position. As to any replacements, the Government Parties shall have **ten (10) days** to object to such proposed selections. A vacancy in either position shall not exist for more than **thirty (30) days**.

**3.8 Security Officer Responsibilities and Duties.** The responsibilities and duties of the Security Officer shall include, at least, each of the following:

- (a) Providing the Government Parties the Annual Report required of Level 3 under Section 4.11 of this Agreement;
- (b) Developing and maintaining Level 3's Information Security Plan, access or disclosure requirements (described in Sections 3.2, 3.3, and 3.4), personnel screening process requirements (described in Sections 3.11 and 3.12), and visitation policy (described in Section 3.13) to promote full compliance with the Agreement;
- (c) Implementing all aspects of compliance with this Agreement and all corporate policies, procedures, and plans to promote and ensure compliance with this Agreement;
- (d) Providing reports to the U.S. Government mandated by the Agreement;
- (e) Being aware of, and reporting to the Government Parties, changes to corporate structure or operations that would reasonably be deemed to have an effect on the terms or operation of the Agreement;
- (f) Being available upon reasonable notice for discussions with the U.S. Government relating to the enforcement of and compliance with the Agreement or any other issue involving national security; and
- (g) Ensuring procedures are in place for Level 3 to comply with Lawful U.S. Process in an expeditious, effective, and unimpeded fashion.

**3.9 Information Security Plan.** Level 3 has previously developed and implemented an information security plan. Following the Effective Date, Level 3 shall maintain or adapt the information security plan to:

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

- (b) ensure assignment of U.S. citizens to positions for which screening is contemplated pursuant to Section 3.11(a);
- (c) assign personnel who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or that regularly deal with information identifiable to such person as Sensitive Information;
- (d) upon request from the Government Parties provide the name, date of birth, and other relevant requested identifier information of each person who regularly handles or deals with Sensitive Information;
- (e) require that personnel handling Classified Information shall have been granted appropriate security clearances, consistent with Executive Order 12968 and other applicable law;
- (f) ensure that the Points of Contact described in Section 3.6 of this Agreement shall have sufficient authority over any employees or contractors of Level 3 who may handle Classified or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;
- (g) ensure that the disclosure of or access to Classified or Sensitive Information is limited to those who have appropriate security clearances and authority;
- (h) Identify the types and positions that require screening pursuant to this Agreement, the required rigor of such screening by type of position, and the criteria by which Level 3 will accept or reject Screened Personnel (as defined in Section 3.11);
- (i) maintain a formal incident response capability with reference to OMB Circular A-130 and NIST Special Publications 800-3, 800-18, and 800-47, or similar national and international standards and frameworks; and
- (j) maintain appropriately secure facilities (*e.g.*, offices, communications centers, network operations centers) within the United States for the handling and storage of any Classified or Sensitive Information.

Level 3 shall make its Information Security Plan and related policies and procedures regarding its information security plan available to the Government Parties upon request.

**3.10 Employee Training.** Level 3 shall instruct and train appropriate officials, employees, contractors, and agents on the security restrictions and safeguards imposed by this Agreement. Level 3 shall make the policies and procedures regarding its employee training available to the Government Parties upon request.

**3.11 Screening of Personnel.** Level 3 shall maintain and implement a screening process to ensure compliance with all personnel screening process requirements agreed to by Level 3

pursuant to this Agreement. The screening process of Level 3 shall cover any existing or newly hired employees and any personnel performing under an agreement with Level 3 in at least the following circumstances:

- (a) The Security Officer; TCO; Points of Contact; all persons who have Access to Classified or Sensitive Information; all persons who have Access to Domestic Communications Infrastructure to monitor the content of Domestic Communications; and all persons who have the ability to monitor personnel with limited access to Domestic Communications under Section 3.11.
- (b) All persons who have Access to Transactional Data, Subscriber Information, CPNI, or personal identifier information; all persons who have limited access to Domestic Communications Infrastructure, excluding the ability to monitor the content of Domestic Communications; and all persons who provision network elements either onsite or remotely. Nothing in this section shall be read to apply the screening requirements in Section 3.12 to Level 3 customers or their agents obtaining their own data.

Upon satisfactory completion of the screening process requirements set forth in this Agreement, such persons shall be considered “**Screened Personnel.**” In addition, Level 3 and will cooperate with any reasonable notice by a U.S. Government Authority to provide additional information necessary for an enhanced background investigation to be conducted by such U.S. Government Authority with respect to Screened Personnel.

**3.12 Screening Process Requirements.** The screening process undertaken pursuant to this Section shall be implemented through a reputable third party, and shall specifically include a background check in addition to a criminal records check. Level 3 shall consult with the Government Parties on the screening procedures utilized by the reputable third party and shall provide to the Government Parties a list of the positions subject to screening no later than **ninety (90) days** after the Effective Date. Level 3 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 Government Parties all the information it collects in its 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 Government Parties, and the candidates shall consent to the sharing of this information with the U.S. Government. In addition:

- (a) Level 3 shall assign U.S. citizens to positions for which screening is contemplated pursuant to Sections 3.11(a);
- (b) Level 3 may Outsource or Offshore positions for which screening is contemplated pursuant to Section 3.11(b). With respect to Outsourced or Offshored personnel, Level 3 shall ensure that such personnel are subject to restricted access methods and background screening requirements under the terms of the Outsourcing or Offshoring arrangements under which they operate in accordance with Section 3.14 of this Agreement. Level 3 shall not Outsource or Offshore functions



involving Access to Classified Information, Sensitive Information, or Lawful U.S. Process;

- (c) Level 3 shall consult with the Government Parties regarding the screening procedures to be used and the positions subject to screening. Level 3 shall reasonably address any concerns the Government Parties may raise with respect to such screening procedures. Level 3 shall use the criteria identified in Section 3.11 of this Agreement to identify the personnel to be screened;
- (d) Level 3 shall cooperate with reasonable requests by the Government Parties, or any U.S. Government Authority desiring to conduct any further background checks;
- (e) Individuals who are rejected pursuant to such further background checks by a U.S. Government Authority shall not be permitted to perform functions that would require screening under this Section. Level 3 shall notify the Government Parties of the job modification of any individual rejected because of the screening conducted pursuant to this Agreement within **seven (7) business days** of such modification, and shall provide the Government Parties upon request with the name, date of birth and any other requested identifier information of such individual;
- (f) Level 3 shall provide annual training programs to instruct Screened Personnel as to their obligations under the Agreement and the need to maintain eligibility under the screening requirements. Level 3 shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements;
- (g) Level 3 shall maintain records relating to the status of Screened Personnel, and shall provide these records, upon request, to any or all of the Government Parties; and
- (h) Any records or other information relating to individual persons provided to or obtained by the Government Parties in connection with this Agreement, including implementation and results of screening requirements, shall be maintained in a secure and confidential manner strictly in accordance with applicable law.

**3.13 Visitation Policy.** No later than **ninety (90) days** after the Effective Date, Level 3 shall adopt and implement a visitation policy for foreign visitors to its Domestic Communications Infrastructure, and shall consult with the Government Parties on the design and implementation of the visitation policy. The visitation policy shall differentiate between different categories of visits based on the sensitivity of the information, equipment, and personnel to which the visitors will have access. The visitation policy shall include the following provisions:

- (a) A requirement to maintain records of any visit requests, including the exact purpose and justification for such request as required under the visitation policy, and any documentation regarding approval or disapproval of such requests, which

shall be maintained by the Security Officer for two (2) years, and shall be made available upon request of the third party auditor or the Government Parties; and

- (b) A requirement that visitors shall at all times be escorted by an employee, with appropriate restrictions on access, set forth by the Security Officer, that are commensurate with the place and purpose of the visit.

**3.14 Outsourcing and Offshoring Control and Access Policy.** No later than **ninety (90) days** after the Effective Date, Level 3 shall adopt and implement an Outsourcing and Offshoring control and access policy and shall negotiate with the Government Parties on the design and implementation of the policy. Level 3 shall not Outsource or Offshore functions covered by this Agreement to an entity that is not within the definition of “Level 3” under this Agreement, except pursuant to the Outsourcing and Offshoring control and access policy. Such policy shall include prior notice of the proposed Outsourcing or Offshoring and the right of the USG Parties to object within **thirty (30) days** of receipt of notice to the proposed Outsourcing or Offshoring. The parties may agree in the policy to exclude classes of Outsourcing or Offshoring contracts of a routine and nonsensitive nature from this notice and approval requirement. All Outsourcing and Offshoring arrangements shall be subject to Level 3’s Outsourcing and Offshoring control and access policy, which shall continue to include logical and physical controls such as restricted access methods and background screening. Level 3 shall not Outsource or Offshore functions involving Access to Classified Information, Sensitive Information, or Lawful U.S. Process.

- (a) Level 3 shall ensure that any entity with which Level 3 has entered into an Outsourcing and Offshoring arrangement complies with Level 3’s Outsourcing and Offshoring control and access policy;
- (b) Level 3 shall include in its contracts with any such entities written provisions requiring that such entities comply with all applicable terms of this Agreement (and otherwise ensure that the entities are aware of, agree to, and are bound to comply with the applicable obligations of the Agreement);
- (c) Level 3 shall notify the Government Parties within **thirty (30) days** of contracting out operation of the Domestic Communications Infrastructure to an entity that is not Level 3, which notice shall identify the name of the entity and the nature of the contract;
- (d) if Level 3 learns that the entity or the entity’s employee has violated an applicable provision of this Agreement, Level 3 shall notify the Government Parties promptly; and
- (e) with consultation and, as appropriate, cooperation with the Government Parties, Level 3 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.

3.15 **Operational Control of NOCs.** Except as set forth in Section 2.1 or otherwise agreed to in writing by the Government Parties, operational control of the Domestic Communications Infrastructure will be restricted to Level 3 NOCs located in the United States. Level 3 will provide the Government Parties with advance notice of any proposed changes in operational control, network control, or Tier support from overseas locations that affect the Domestic Communications Infrastructure. The Government Parties shall have the right to review and object to such changes.

3.16 **Operational Control of Cable Systems.** Level 3 shall have the ability to promptly and effectively interrupt in whole or in part traffic to and from the United States on each Cable System by disabling or disconnecting circuits at the U.S. cable landing or at other locations within the United States. Level 3 shall also have the ability to isolate any U.S. NOC, U.S. cable landing station, or the connecting cable segment from the rest of the Cable System, and shall also have the ability to override the United Kingdom NOC as indicated in 2.1(f). Level 3 will provide the Government Parties with advance notice of any actions to be taken in accordance with this provision. If Level 3 takes any actions in accordance with this provision in an emergency situation, Level 3 will notify the Government Parties within **five (5) business days**.

3.17 **Nondisclosure of Protected Data.** In carrying out the responsibilities set forth in this Agreement, the Security Officer and/or the Points of Contact shall not disclose directly or indirectly any information concerning Lawful U.S. Process, Classified Information, or Sensitive Information to any third party, or to any officer, director, shareholder, employee, agent, or contractor of Level 3, including those who serve in a supervisory, managerial or executive role with respect to the employees working with the information unless disclosure has been approved by prior written consent obtained from the Government Parties or there is an official need for disclosure of the information in order to fulfill an obligation consistent with the purpose for which the information is collected or maintained.

3.18 **Notice of Obligations.** Level 3 shall instruct appropriate officials, employees, contractors, and agents as to their obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in Article 4 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.19 **Access to Classified or Sensitive Information.** Nothing contained in this Agreement shall limit or affect the authority of a U.S. Government Authority to deny, limit, or revoke whatever access that Level 3 might have to Classified or Sensitive Information under that Government Authority's jurisdiction.

#### **ARTICLE 4: REPORTING AND NOTICE**

4.1 **Filings Concerning *de jure* or *de facto* Control of Level 3.** If Level 3 makes any filing with the FCC or any other Government Authority relating to the *de facto* or *de jure* control of Level 3 except for filings with the FCC for assignments or transfers of control to any entity that is within the definition of "Level 3" under this Agreement that are pro forma, Level 3 shall promptly provide to the Government Parties written notice and copies of such filing.

4.2 **Change in Control.** If the Security Officer, TCO, or any member of the Management of Level 3 acquires any information that reasonably indicates that any foreign entity or individual has or will likely gain either: (i) Control; or (ii) *de facto* or *de jure* control of Level 3 then such person shall notify the Security Officer, who in turn, shall promptly report to the Government Parties in writing within **five (5) business days** after such person acquires such information. Awareness of any the following shall trigger this notice obligation:

- (a) Any increase in ownership of Level 3 by ST Telemedia in excess of 34.5 percent;
- (b) Any additional ownership of Level 3 by the Government of Singapore via any entity other than ST Telemedia, at any percentage; or
- (c) Any additional foreign ownership that would result or likely result in a foreign person owning a more than a ten percent (10%) (direct or indirect) interest in Level 3 or in *de facto* or *de jure* control of Level 3.

The Security Officer shall submit reports required under this Section in writing no later than **five (5) business days** after receipt of such knowledge and the Security Officer's report shall, at a minimum: identify the entity or individual(s) providing the notice (specifying the name, addresses, and telephone numbers of the entity); (ii) identify the beneficial owners of the increased or prospective increased interest in Level 3 or any of the Cable Systems 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 that the entity or individual(s) has or will likely obtain in Level 3 or any of the Cable Systems and, if applicable, the basis for their prospective Control of Level 3 or any of the Cable Systems.

4.3 **Joint Ventures.** Level 3 shall provide notification of any joint venture with a non-U.S. party under which the joint venture or non-U.S. party may provide Domestic Communications at least **sixty (60) days** before consummation.

4.4 **Notice of Foreign Influence.** If the Security Officer, TCO, or any member of Management of Level 3 acquires any information that reasonably indicates that any foreign government, any foreign-government-controlled entity, or any foreign entity:

- (a) plans to participate, or has participated, in any aspect of the day-to-day management of Level 3 in such a way that interferes with or impedes the performance by Level 3 of its duties and obligations under the terms of this Agreement; or
- (b) plans to exercise, or has exercised, as a direct or indirect shareholder of Level 3, any control of Level 3 in such a way that interferes with or impedes the performance by Level 3 of its duties and obligations under the terms of this Agreement;

such person shall promptly report to the Security Officer, who in turn, shall within 24 hours report to the Government Parties in writing of the timing and nature of the foreign government's or entity's plans and/or actions.

**4.5 Procedure and Process on Reporting.** Within **forty-five (45) calendar days** after the Effective Date, Level 3 shall adopt and distribute to its Management and the Security Officer a written procedure or process for the reporting by the Security Officer to the Government Parties of noncompliance with this Agreement. This written procedure or process shall also provide for the reporting by employees, agents and contractors to the Security Officer of information that must be reported to the Government Parties under this Article. Any violation by Level 3 of any material term of such corporate policy shall constitute a breach of this Agreement. By a written statement, Level 3 shall notify all employees, contractors, and agents that the general categories of information identified in this Article should be disclosed to the Security Officer and shall be set forth in a clear and prominent manner the contact information for the Security Officer to whom such information shall be reported. Level 3 shall make such process or procedure documents available to the Government Parties upon request.

**4.6 Non-Retaliation.** Within **forty-five (45) calendar days** after the Effective Date, Level 3 shall adopt and distribute to its Management an official corporate policy that strictly prohibits discrimination or any adverse action against any officer, director, employee, contractor, or agent because he or she has in good faith initiated or attempted to initiate a notice or report under this Article, or has notified or attempted to notify the Security Officer to report information that he or she believes in good faith is required to be reported to the Government Parties under either this Article or under the written statement of Level 3 to employees on the reporting of any such information. Any violation by Level 3 of any material term of such corporate policy shall constitute a breach of this Agreement. Level 3 shall make such process or procedure documents available to the Government Parties upon request.

**4.7 Reporting of Incidents.** Level 3 shall report to the Government Parties any information acquired by any of the officers, directors, employees, contractors, or agents of Level 3 that reasonably indicates:

- (a) a breach of this Agreement;
- (b) access to or disclosure of Domestic Communications, or the conduct of Electronic Surveillance, in violation of federal, state or local law or regulation;
- (c) access to or disclosure of CPNI or Subscriber Information in violation of federal, state or local law or regulation (except for violations of FCC regulations relating to improper commercial use of CPNI); or
- (d) improper access to or disclosure of Classified or Sensitive Information.

The Security Officer shall make this report in writing by the appropriate officer to the Government Parties no later than **five (5) calendar days** after Level 3 acquires information indicating a matter described in this Section. Level 3 shall lawfully cooperate in investigating

the matters described in this Section. Level 3 need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

**4.8 Access to Information and Facilities.** A Government Party, or another agency or personnel assigned to assist a Government Party, may visit at any time and with thirty (30) minutes' notice any facilities of Level 3 to conduct on-site reviews concerning the implementation of the terms of this Agreement and Level 3 shall provide unimpeded access to information concerning technical, physical, management, or other security measures needed by the Government Parties to verify compliance with the terms of this Agreement.

**4.9 Access to Personnel.** Upon reasonable notice from a Government Party, or from another agency or personnel assigned to assist a Government Party, Level 3 shall make available for interview any personnel and require contractors to make available appropriate personnel available in the United States who are in a position to provide information to verify compliance with the terms of this Agreement.

**4.10 Audit Requirement.** Level 3 shall retain and pay for a neutral third party to complete an assessment of the vulnerabilities associated with ensuring domestic control of Level 3's Domestic Communications Infrastructure and an audit that objectively assesses Level 3's compliance with this Agreement. Within **sixty (60) days** from the Effective Date, Level 3 shall provide notice of the proposed auditor, and the Government Parties shall have an opportunity to provide reasonable objections to the selection of the auditor within **sixty (60) days** of receipt of such notification. The Government Parties shall be consulted on the scope of the vulnerability assessment and the audit. The vulnerability assessment shall be initiated within **sixty (60) days** of the date the auditor is selected. The initial audit will be due one (1) year from the Effective Date. The Government Parties shall maintain the right to request additional audits as determined by the Government Parties. Subsequent audit requests from the Government Parties will not exceed one (1) audit per year. Level 3 shall ensure that the vulnerability assessment and all reports generated by the auditor are promptly provided to the Government Parties.

**4.11 Annual Report.** On or before the last day of February of each year, Level 3 shall submit to the Government Parties a report assessing the compliance of Level 3 with the terms of this Agreement for the preceding calendar year. The report shall include:

- (a) a copy of the then current policies and procedures adopted to comply with this Agreement;
- (b) a summary of the changes, if any, to the policies or procedures, and the reasons for those changes;
- (c) a summary of any known acts of noncompliance with the terms of this Agreement, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future;

- (d) identification of any other issues that, to the knowledge of Level 3, will or reasonably could affect the effectiveness of or its compliance with this Agreement;
- (e) a list of companies that performed any maintenance, repair, or replacement that resulted in any material modification to the Principal Equipment, or systems or software used with the Principal Equipment, for the Cable System infrastructure;
- (f) updates to undersea cable networks Principal Equipment with associated system/software produces necessary to operate the Principal Equipment;
- (g) updates to the U.S. Cable System Contracts List;
- (h) a copy of all audit reports compiled by the third-party auditor conducted pursuant to this Agreement under Section 4.10; and
- (i) updates to network and telecommunications architecture.

4.12 **Notice of Establishment of Additional NOCs.** In the event that Level 3 establishes a new NOC, Level 3 shall provide prior written notice of such establishment to the Government Parties at least **thirty (30) days** prior to the commencement of such NOC operations.

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

Department of Homeland Security  
Assistant Secretary for Policy  
Washington, D.C. 20528  
Email: ip-fcc@dhs.gov

Department of Justice  
Assistant Attorney General for National Security  
National Security Division  
ATTN: Foreign Investment Review Staff  
950 Pennsylvania Avenue, NW  
Washington, D.C. 20530  
Email: FIRS-TT@usdoj.gov

Department of Defense Chief Information Officer  
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

Level 3 Communications, Inc.  
Attn: Dwight Steiner  
1025 Eldorado Boulevard  
Broomfield, Colorado 80021  
Fax: (720) 567-2285  
Email: dwight.steiner@level3.com

With a copy to Level 3's legal counsel:

Level 3 Communications, Inc.  
Attn: Chief Legal Officer  
1025 Eldorado Boulevard  
Broomfield, Colorado 80021  
Fax: (720) 888-5127

Kent Bressie  
Wiltshire & Grannis LLP  
1200 18th Street, N.W., Suite 1200  
Washington, D.C. 20036-2516  
Fax: (202) 730-1301  
Email: kbressie@wiltshiregrannis.com

## **ARTICLE 5: FCC CONDITION**

5.1 **FCC Approval.** Upon the execution of this Agreement by the Parties, the Government Parties on their own motion at an appropriate time or at the request of Level 3 shall 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 Government Parties have no objection to the FCC's grant of the pending Applications and Petition described in the Recitals of this Agreement. This Section is effective upon the Effective Date, provided however, that in the case of a material modification or withdrawal of the Application after the execution of this Agreement the effectiveness of this Section may be suspended by a Government Party, and any such FCC filing is subject to the right to object reserved in Section 5.2 of this Agreement.

5.2 **Right to Object to Future FCC Filings.** Level 3 agrees that in any application or petition to the FCC for licensing or other authority related to Domestic Communications Infrastructure or to any Cable System filed with or granted by the FCC after the execution of this Agreement, except with respect to *pro forma* assignments or *pro forma* transfers of control, Level 3 shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 7.8, the Government Parties reserve the right to object, formally or informally, to the grant of any other FCC application or petition of Level 3 for a license or other authorization under Titles II and III of the



Communications Act of 1934, as amended, and to seek additional or different terms that would, consistent with the public interest, address any threat to the ability of the United States to enforce the laws, preserve the national security and protect the public safety raised by the services and transactions underlying any such application or petition.

## **ARTICLE 6: DISPUTES**

**6.1 Informal Resolution.** The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. Disagreements shall be addressed, in the first instance, at the staff level by the Parties' designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to the legal counsel for Level 3, the Assistant Attorney General for National Security of DOJ, the Assistant Secretary for Policy of DHS, Department of Defense Chief Information Officer, or their respective designees, unless the Government Parties believe that important national interests can be protected, or Level 3 believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 6.2 of this Agreement. If, after meeting with higher authorized officials, a Party determines that further negotiation would be fruitless, then that Party may resort to the remedies set forth in Section 6.2 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.

**6.2 Enforcement of Agreement.** Subject to Section 6.1 of this Agreement, if any Government Party believes that Level 3 has breached or is about to breach this Agreement, the Government Party may bring an action against Level 3 for appropriate judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. Government Agency to:

- (a) require that the Party believed to have breached, or about to breach, this Agreement cure such breach within **thirty (30) calendar days**, or whatever shorter time period is appropriate under the circumstances, upon receiving written notice of such breach;
- (b) request that the FCC modify, condition, revoke, cancel, or render null and void any license, permit, or other authorization granted or given by the FCC to Level 3, request that the FCC take other action, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against Level 3;
- (c) seek civil sanctions for any violation by Level 3 of any U.S. law or regulation or term of this Agreement;
- (d) pursue criminal sanctions against Level 3, or any director, officer, employee, representative, or agent thereof, or against any other person or entity, for violations of the criminal laws of the United States; or
- (e) seek suspension or debarment of Level 3 from eligibility for contracting with the U.S. Government, in accordance with applicable law and regulation.

6.3 **Irreparable Injury.** Level 3 agrees that the United States would suffer irreparable injury if for any reason Level 3 failed to perform any of its obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, Level 3 agrees that, in seeking to enforce this Agreement, the Government Parties shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

6.4 **Waiver.** The availability of any civil remedy under this Agreement shall not prejudice the exercise of any other civil remedy under this Agreement or under any provision of law, nor shall any action taken by a Party in the exercise of any remedy be considered a waiver by that Party of any other rights or remedies. The failure of any Party to insist on strict performance of any of the provisions of this Agreement, or to exercise any right they grant, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by any Party of any provision or right shall be valid unless it is in writing and signed by the Party.

6.5 **Waiver of Immunity.** Level 3 agrees, to the extent that they or any of their property (including FCC licenses and authorizations and intangible property) is or becomes entitled at any time to any immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of Government from any legal action, suit or proceeding or from setoff or counterclaim relating to this Agreement, from the jurisdiction of any competent court or the FCC, from service of process, from attachment prior to judgment, from attachment in aid of execution of a judgment, from execution pursuant to a judgment or arbitral award, or from any other legal process in any jurisdiction, they, for themselves and their respective property expressly, irrevocably and unconditionally waive, and agree not to plead or claim, any such immunity with respect to matters arising with respect to this Agreement or the obligations herein (including any obligation for the payment of money) in any proceeding brought by a U.S. federal, state, or local Government Authority. Level 3 agrees that the waiver in this provision is irrevocable and is not subject to withdrawal in any jurisdiction or under any statute, including the Foreign Sovereign Immunities Act, 28 U.S.C. § 1602 *et seq.* The foregoing waiver shall constitute a present waiver of immunity at any time any action is initiated by a U.S. federal, state, or local Government Authority against Level 3 with respect to compliance with this Agreement.

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

## ARTICLE 7: OTHER

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

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

7.3 **Other Laws.** Nothing in this Agreement is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local laws on Level 3, (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority the U.S. Government may possess over the activities or facilities of Level 3 located within or outside the United States (including authority pursuant to the International Emergency Economic Powers Act). Nothing in this Agreement is intended to or is to be interpreted to require the Parties to violate any applicable U.S. law.

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

7.5 **Modifications.** This Agreement may only be modified by written agreement signed by all Parties. The Government Parties agree to consider promptly and in good faith possible modifications to this Agreement if Level 3 believes that the obligations imposed on it under this Agreement are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, and public safety concerns. Any substantial modification to this Agreement shall be reported to the FCC within **thirty (30) calendar days** after approval in writing by the Parties.

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

7.7 **Changes in Circumstances for Level 3.** The Government Parties agree to negotiate in good faith and promptly with respect to any request by Level 3 for relief from application of specific provisions of this Agreement if there is a change in circumstances such that those provisions become unduly burdensome or have a demonstrably adverse effect on the competitive position of Level 3.

7.8 **Changes in Circumstances for the Government Parties.** If after the date that the Parties have executed this Agreement, a Government Party finds that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns, then Level 3 will negotiate in good faith to modify this Agreement to address those concerns.

7.9 **Termination of Agreement.** This Agreement may be terminated at any time by a written agreement signed by the Parties. The Parties agree that they will reasonably consider any termination request submitted pursuant to this Agreement.

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

7.11 **Successors and Assigns.** This Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns. This Agreement shall also be binding on all subsidiaries, divisions, departments, branches, and other components or agents of Level 3.

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

*[Signature Pages Follow]*

This Agreement is executed on behalf of the Parties:

**Level 3 Communications, Inc.**

Date: 23 September 2011

By: 

Printed Name: Thomas C. Stortz

Title: Executive Vice President

**Department of Homeland Security**

Date: 26 September 2011

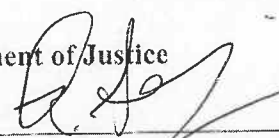
By: 

Printed Name: SHAWN B. COOLEY

Title: Director, Foreign Investment Risk Mgt  
Office of Policy

**Department of Justice**

Date: 26 September 2011

By: 

Printed Name: Richard C. Sofield

Title: Director, Foreign Investment Review Staff

**Department of Defense**

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

This Agreement is executed on behalf of the Parties:

**Level 3 Communications, Inc.**

Date: 23 September 2011

By: 

Printed Name: Thomas C. Stortz

Title: Executive Vice President

**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Department of Defense**

Date: 26 Sept 11

By: 

Printed Name: Ronald J. Casey

Title: Deputy CIO

## EXHIBIT A

### CONDITION TO FCC AUTHORIZATION

**IT IS FURTHER ORDERED**, that this order and authorization and any licenses or authorizations granted hereunder are subject to compliance with the provisions of the agreement (the “Agreement”) between **Level 3 Communications, Inc.**, including its subsidiaries and affiliates, on the one hand, and the U.S. Department of Justice, the U.S. Department of Homeland Security, and the U.S. Department of Defense (collectively, “**Government Parties**”) on the other, dated [\_\_\_\_\_], which Agreement is designed to address national security, law enforcement, and public safety concerns of the Government Parties regarding the authority granted herein. Nothing in the Agreement is intended to limit any obligation imposed by federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC’s implementing regulations.