

NATIONAL SECURITY AGREEMENT

This National Security Agreement (“**Agreement**” or “**NSA**”) is made as of the date of the last signature affixed hereto, (“**Effective Date**”) by and between PT Telekomunikasi Indonesia Tbk. (“**PT Telkom**”), its subsidiary PT Telekomunikasi Indonesia International (“**Telin**”), and Telin’s United States subsidiary Telekomunikasi Indonesia International (USA), Inc. (“**Telkom USA**” and, collectively, with PT Telkom and Telin, the “**Telkom Parties**”), on the one hand, and the United States Department of Justice (“**DOJ**,” and, together with the Telkom Parties, the “**Parties**”), on the other hand.

RECITALS

WHEREAS, United States (“**U.S.**”) communication systems are essential to the ability of the United States Government (“**USG**”) 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 USG has an obligation to the public to ensure that communications in the United States and related information regarding the provisioning, servicing, and support of such communications are secure in order to protect the privacy of United States persons, to preserve the security of the nation, 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 13,231, Critical Infrastructure Protection in the Information Age and Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (February 12, 2013));

WHEREAS, the protection of Classified and Sensitive Information also is critical to United States national security;

WHEREAS, Telkom USA, a Delaware corporation with its headquarters at 800 Wiltshire Blvd, 6th Floor, Suite 620, Los Angeles, CA 90017, desires a Federal Communications Commission (“**FCC**” or “**Commission**”) authorization to provide international global or limited global facilities-based and resold services to all international points in order to provide wholesale telecommunication transport to support third-party carrier Voice, Data, Mobile Internet, and other services, including Data Connectivity, for enterprise users, including, but not limited to, Indonesian companies in the U.S. and U.S. companies with offices in Indonesia;

WHEREAS Telkom USA, which currently has no plans to provide end-user telecommunications services, other than wholesale service to carriers and enterprise-level subscribers as stated in Telkom USA’s December 23, 2015 submission to the DOJ, the U.S. Department of Homeland Security, and the U.S. Department of Defense (Team Telecom),

acknowledges that, upon receiving the FCC authority at issue, it would have the authority to offer end-user services;

WHEREAS, Telin, Telkom USA's parent entity and a subsidiary of PT Telkom, the Indonesian-government majority-owned incumbent telecommunications provider in Indonesia, and PT Telkom collectively and indirectly operate through their subsidiaries as providers of telecommunications and broadband services in a range of markets throughout the world, and intend to so operate indirectly through Telkom USA;

WHEREAS on September 19, 2014, Telkom USA filed an application with the FCC under Section 214 of the Communications Act of 1934, Title 47 U.S. Code, as amended, and pursuant to Sections 63.18(e)(1) and (2) of the Commission's rules, Title 47, Code of Federal Regulations (FCC File No. ITC-214-20140918-00265), seeking approval for Global or Limited Global Facilities-Based authority and Global or Limited Global Resale authority ("**the FCC Application**");

WHEREAS, Telkom USA directly will have, and PT Telkom and Telin indirectly will have, physical and electronic (e.g., logical) access to U.S. critical infrastructure and to customer and end-user information that may be subject to U.S. privacy and electronic surveillance, physical search, and storage laws;

WHEREAS, there are no current plans for PT Telkom and Telin to have physical or electronic (logical) access to U.S. critical infrastructure or Domestic Communications Infrastructure as described herein, but allowing that, in the future, those plans might change, and considering the potential for such access to exist indirectly or in a manner not currently foreseen or appreciated by the Telkom Parties;

WHEREAS, there are no current plans for PT Telkom or Telin to have physical or electronic (logical) access to customer and end-user information that is subject to U.S. privacy and electronic surveillance, physical search, and storage laws, but allowing that, in the future, those plans might change, and considering the potential for such access to exist indirectly or in a manner not currently foreseen or appreciated by the Telkom Parties;

WHEREAS, the Telkom Parties either have and will continue to have, or may in the future have, obligation(s) to protect from unauthorized disclosure the contents of wire and electronic communications to and from the United States under United States law;

WHEREAS, the DOJ has identified national security, law enforcement, and public safety concerns which are addressed through the execution of this Agreement;

WHEREAS, PT Telkom, Telin and Telkom USA are willing to enter into this Agreement; and

NOW, THEREFORE, the Parties enter into this Agreement to address the DOJ's national security, law enforcement, and public safety concerns.

ARTICLE I DEFINITIONS

As used in this Agreement and the Implementation Plan:

- 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, etc.).
- 1.2 **“Call Associated Data”** means any information relating to a communication or relating to the sender or recipient of that communication and may include, without limitation, subscriber identification, called party number or other identifier, calling party number or other identifier, 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 digits, in-band and out-of-band signaling, and party add, drop and hold, and any other “call identifying information,” as defined in 47 U.S.C. § 1001(2), as amended or superseded.
- 1.3 **“Call Detail Record” (“CDR”)** means the data records or call log records that contain information about each Call made by a user and processed by switch, call manager, or call server.
- 1.4 **“Classified Information”** means any information determined pursuant to Executive Order 13,526, as amended or superseded, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.
- 1.5 **“Control” and “Controls”** means the power, direct or indirect, 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, make, reach, or cause decisions for such entity 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; or
- (f) obligations under this Agreement.

1.6 **“Customer Proprietary Network Information (“CPNI”)** means:

- (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship;
- (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; and/or
- (c) information falling within the definition given in 47 U.S.C. § 222(h)(1).

1.7 **“De facto” and “de jure”** control have the meaning provided in 47 C.F.R. § 1.2110, as amended or superseded.

1.8 **“DOJ”** has the meaning given it in the Preamble.

1.9 **“Domestic Communications” (or, “DC”)** means:

- (a) Wire Communications or Electronic Communications (whether stored or not) between one U.S. location and another U.S. location; or
- (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates from or terminates at a U.S. location.

1.10 **“Domestic Communications Infrastructure” (or, “DCI”)** means:

- (a) the transmission and switching equipment (including hardware, software, and upgrades) leased or owned by or on behalf of PT Telkom, Telin, or Telkom USA to provide, process, direct, control, supervise or manage DC;
- (b) facilities and equipment leased or owned by or on behalf of PT Telkom, Telin, or Telkom USA that are physically located in the United States; and

- (c) the facilities and equipment leased or owned by or on behalf of any PT Telkom, Telin, or Telkom USA U.S. subsidiaries to control the equipment or facilities described in (a) and (b) above.
 - (d) The phrase “on behalf of” as used in this section does not apply to facilities or equipment of entities (with the exception of subsidiaries of the Telkom Parties) with which the Telkom Parties have contracted for, and used by such entities to provide, peering, interconnection, roaming, long distance, or other communications service, including transport, or to other similar arrangements on which the Parties may agree. Further, without limitation, DCI shall not be construed to include equipment dedicated to the termination of international submarine cable systems, including systems that terminate at one or more non-U.S. points, provided that such equipment is used solely to effectuate the operation of such submarine cable systems and in no manner controls land-based transport network(s) or their associated systems in the United States.
- 1.11 **“Effective Date”** has the meaning given it in the Preamble.
- 1.12 **“Electronic Communication”** has the meaning given it in 18 U.S.C. § 2510(12), as amended or superseded.
- 1.13 **“Electronic Surveillance”** means:
- (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, as amended or superseded, and electronic surveillance as defined in 50 U.S.C. § 1801(f), as amended or superseded;
 - (b) Access to or support of stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*, 18 U.S.C. § 2510(17), and 50 U.S.C. § 1821(5), as amended or superseded;
 - (c) the acquisition of dialing 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.*, as amended or superseded;
 - (d) the acquisition of location-related information concerning a telecommunications service subscriber;
 - (e) the preservation of any of the above information pursuant to 18 U.S.C. § 2703(f), as amended or superseded; and
 - (f) including the Access to, or the acquisition or interception of, communications or information as described in (a) through (e) above, and comparable State laws.

- 1.14 **“FCC”** has the meaning given it in the Recitals.
- 1.15 **“FCC Application”** has the meaning given in the Recitals.
- 1.16 **“Foreign”**, where used in this Agreement, whether capitalized or lower case, means non-U.S.
- 1.17 **“Governmental Authority” or “Governmental Authorities”** means:
- (a) any government;
 - (b) any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau, or political subdivision; and
 - (c) any court, tribunal, judicial or arbitral body.
- 1.18 **Implementation Plan** means a forthcoming document that outlines the written policies, standards, and procedures that the Telkom Parties will implement in order to comply with their respective obligations under this Agreement, subject to the DOJ’s approval. Certain of the rights and obligations of the Parties will be set forth in further detail in the Implementation Plan, which will be drafted, adopted, and implemented by PT Telkom, Telin, and/or Telkom USA in accordance and consistent with this Agreement pursuant to the Section 2.1 of this NSA. PT Telkom, Telin, and/or Telkom USA shall comply with the Implementation Plan as it applies to each with respect to their obligations hereunder, which may be amended from time to time pursuant to Article VIII.
- 1.19 **“Intercept,” “Interception,” or “Intercepted”** has the meaning defined in 18 U.S.C. § 2510(4), as amended or superseded.
- 1.20 **“Internet Protocol Detail Record” (“IPDR”)** means a streaming data protocol used by Operations Support Systems (“OSS”) and Business Support Systems (“BSS”) to collect and record a user’s data traffic statistics on a network. IPDR mainly is used by cable industries and incorporated into Cablelabs Data Over Cable Service Interface Specification (“DOCSIS”) protocol.¹ It provides network usage and user information for the network management.
- 1.21 **“Lawful U.S. Process”** means U.S. federal, state, or local electronic surveillance orders or authorizations, and other orders, legal process, statutory authorizations and certifications for interception of, Access to, or disclosure of DC, and Call Associated Data, Transactional Data, or Subscriber Information that are authorized by U.S. law, including the orders of the President in the exercise of his/her authority under the Constitution, federal statutes and regulations, and other executive authorities, to include, without limitation, Section 706 of the Communications Act of 1934, as amended (47 U.S.C. § 606), Section 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and

¹ DOCSIS is a standard interface for cable modems.

Executive Order 11161 (as amended by Executive Order 11382), and 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.*).

- 1.22 **“Managed Network Service Provider”** means any third party using an end-to-end or managed-services platform to provide any of the following functions for DCI, if any: operations and management support; corrective and preventative maintenance including intrusive testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, and development, and the implementation of changes and upgrades.
- 1.23 **“Network Operations Center” or “NOC”** means the locations and facilities designated to perform network management, monitoring, maintenance, provisioning, or other operational functions for DCI in the United States.
- 1.24 **“Offshore” or “Offshoring”** means, with respect to DC, performing obligations of this Agreement through the use of entities and personnel outside the territorial limits of the U.S., whether those entities or personnel are employees of PT Telkom, Telin, or Telkom USA, or are third parties.
- 1.25 **“Outsource” or “Outsourcing”** means, with respect to DC, supporting the services and operational needs of PT Telkom, Telin, or Telkom USA at issue in this Agreement through the use of contractors or third parties.
- 1.26 **“Parties”** has the meaning given it in the Preamble. “Party,” singular, means any neutral sole entity that comprises one of the entities within the Parties.
- 1.27 **“Personal Identifiable Information” (“PII”)** means the name and aliases, social security number, date of birth, place of birth, citizenship status, contact information, and current address of an individual.
- 1.28 **“Principal Equipment”** means:
- (a) the primary electronic components of or supporting a mobile or fixed communication network, broadband network, transport and fiber network, and terrestrial wireless/satellite networks;
 - (b) softswitches;
 - (c) network routers;
 - (d) call managers/servers; and

- (e) any firmware necessary for the proper operation of (a), (b), (c), and (d), with the exception of software used for common business functions (e.g. Microsoft Office).²

1.29 **“PT Telkom”** has the meaning given in the Preamble;

1.30 **“Screened Personnel”** means those persons described in detail in Article IV, Section 4.13 of this Agreement.

1.31 **“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;
- (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; and
- (f) other information that is not Classified Information and that is marked expressly as “Sensitive Information” by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency.

1.32 **“Subscriber Information”** means information:

- (a) of the type referred to and accessible subject to the procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709, as amended or superseded;
- (b) sought pursuant to the provisions of other Lawful U.S. Process.

1.33 **“Telin”** has the meaning given in the Preamble;

² Principal Equipment shall include hardware used for a NOC, satellite, earth station, enhanced packet core (“**EPC**”), broadcast, or cell-site station, and the electronic equipment necessary for the operation of the base station control units (“**BSC**”), digital TV transmitters, network routers, call servers, circuit switches/softswitches, wired and wireless radio transmitters, and multiplexers, as applicable. Examples of some Principal Equipment are gateway routers, access routers, home location registers, visitor location registers, smart antennas, software defined radios, call servers, evolved Node B (“**eNodeB**”), submarine line terminals, optical add-drop multiplexers, mobile switches, circuit switches, Softswitches, private branch exchanges (“**PBXs**”), microwave radios, and other equipment or firmware meeting the criteria set forth in Section 1.28(a) through (e).

- 1.34 **“Telkom USA”** has the meaning given it in the Preamble, to include any of that entity’s subsidiaries.
- 1.35 **“Trade Secret”** has the meaning provided in 18 U.S.C. § 1839(3).
- 1.36 **“Transactional Data”** means:
- (a) any “call identifying information,” as defined in 47 U.S.C. § 1001(2), as amended or superseded, including, without limitation, the telephone number or similar identifying designator associated with a communication;³
 - (b) an Internet address or similar identifying designator associated with a communication;
 - (c) the time, date, size, and duration of a communication;
 - (d) any information relating specifically to the identity and physical/logical address of a subscriber, user, or account payer of Telkom USA;
 - (e) to the extent associated with a subscriber, user, or account payer of Telkom USA, any information relating to telephone numbers, Internet addresses, e-mail accounts, text messages, Instant Messages (**“IMs”**) or similar identifying designators, to include the physical location of equipment, if known and if different from the location information provided under (f), below, and the types of service, length of service, fees, and usage, including CDRs, CPNI, and any other billing records; and
 - (f) any information indicating the physical location to or from which a communication is transmitted.
- 1.37 **“United States” (or “U.S.”)** means the United States of America, including all of its States, districts, territories, possessions, commonwealths, and territorial and special maritime jurisdictions.
- 1.38 **“United States (or U.S.) Law”** means any U.S. federal, state, or local law or regulation.
- 1.39 **“U.S. Point of Presence” (“U.S. POP”)** means a physical location in the United States where PT Telkom, Telin, or Telkom USA, as applicable, permits access to its network facilities located in the United States. U.S. POPs include, but are not be limited to, site(s) supporting the termination, origination, mediation, routing, and/or switching of DC and equipment physically located in the United States, in such a manner as to provide real-time routing of all DC.

³ Also includes Uniform Resource Locators (**“URLs”**) and Internet Protocol (**“IP”**) address/header information.

- 1.40 **“Wire Communication”** has the meaning given it in 18 U.S.C. § 2510(1), as amended or superseded.
- 1.41 **“Other Definitional Provisions”**: Other capitalized terms used in this Agreement and the Implementation Plan 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, feminine, and gender-neutral versions of such terms. Whenever the words “include,” “includes,” or “including” are used in this Agreement, they shall be deemed to be followed by the words “without limitation.” Where a term is specifically defined herein, that definition controls over other definitions, general industry terms of art, or common understandings regarding the meaning for such term.

ARTICLE II

OPERATIONS, FACILITIES, INFORMATION STORAGE, AND ACCESS

- 2.1 **Implementation Plan**: The Telkom Parties will create an Implementation Plan regarding the methods and processes that will be used to ensure compliance with the NSA, and as outlined and defined in Section 1.18 of this Agreement. Such Implementation Plan is subject to DOJ approval and is due to the DOJ for its review within **one hundred fifty (150) days** of the Effective Date.
- (a) The Implementation Plan must require Telkom USA to prepare network security policy documents subject to DOJ approval for the matters of interest herein; specifically, information security, remote access, encryption, physical security, cybersecurity, third-party contractors, outsourcing/offshoring, and system logs.
 - (b) The Implementation Plan will include additional requirements and specifications not specified herein, but which support the interests and intent identified in this Agreement (*e.g.*, additional deadline periods). Any such requirements and specifications will become part and parcel of the obligations memorialized in this Agreement once the Implementation Plan is approved and adopted.
 - (c) The Implementation Plan is deemed adopted once the Parties all agree on its terms and have executed a final copy. The Implementation Plan’s Adoption Date shall be the date of the last signature affixed thereto. Until such time as the Implementation Plan is adopted, the terms of this NSA shall control.
- 2.2 **Operational Requirements**: With respect to the operation of DCI, the Telkom Parties agree as follows, except where otherwise approved by the DOJ:
- (a) **Point of Presence**: DC shall be routed through U.S. POPs, or otherwise through a third-party point of presence (“**POP**”) in the United States, in accordance with the Implementation Plan (as defined herein) so that, pursuant to Lawful U.S. Process, Electronic Surveillance can be conducted. To the extent that DC are

routed through a U.S. POP, the Telkom Parties will provide any technical or other assistance required to accomplish such Electronic Surveillance.

- (b) **DCI**: All Principal Equipment used for DC shall be located in the United States, except as otherwise permitted under the terms of this NSA or policies adopted in accordance herewith. All DCI shall be managed, directed, controlled, supervised, provisioned, and maintained in accordance with this NSA's terms.
- (c) **Network Operation Center**: NOCs supporting DC or DCI shall be maintained and remain within the United States. The manpower operation or support of such NOCs shall exclusively be performed by Screened Personnel, as defined herein. Should it be necessary to rely upon subcontractors or third parties to operate or support such NOCs, such subcontractors or third parties will be subject to pre-approval by the DOJ in accordance with relevant subsections of this Agreement.
 - 1) Within **forty-five (45) days** of the Effective Date, Telkom USA shall submit to the DOJ a notice of the location(s) of all NOCs supporting DC or DCI.
 - 2) Thereafter, should PT Telkom, Telin, or Telkom USA begin reliance upon a new NOC location to support DC or DCI, that location shall be notified to the DOJ within **thirty (30) days** of such reliance.
- (d) **Exclusion of Foreign-Based Control over DCI**: The Telkom Parties must continue to maintain DC or DCI for the U.S. and its territories that is exclusively controlled, managed, and operated from the U.S. and its territories.
 - 1) Any support of DC or DCI relying upon any facility or service outside the U.S. and its territories, including facilities or equipment providing remote access to DC or DCI, must be pre-approved by the DOJ, with the understanding that such facility or service is subject to the terms of this NSA to the extent it supports DC or DCI.
 - 2) PT Telkom, Telin, and/or Telkom USA shall notify the DOJ of the intentions to use such facilities or services described in Section 2.2(d) located outside the U.S. at least **sixty (60) days** in advance, and the DOJ shall have **forty-five (45) days** after such notice to review and object to the same. Should the DOJ object, the facility or service at issue will not be utilized to support DC or DCI; where there is no objection from the DOJ within that **forty-five (45) day** period, use of such facility or service will be permitted and otherwise be subject to the terms and strictures of this NSA.

- 2.3 **CPNI**: The Telkom Parties shall comply with all applicable FCC rules and regulations governing Access to and the storage of CPNI.

- 2.4 **Compliance with Lawful U.S. Process:** All reasonable steps shall be taken to configure DCI to support, and to ensure that Telkom USA is capable of effecting, in an effective, efficient, and unimpeded fashion, compliance with Lawful U.S. Process.
- (a) Compliance with Lawful U.S. Process by the Telkom Parties, as applicable, shall be effected from within the United States.
 - (b) The Telkom Parties shall ensure in any agreements with other carriers regarding such carriers' reliance upon the DCI that Lawful U.S. Process is recognized and facilitated.
 - (c) The Law Enforcement Point of Contact (LE POC), as defined herein, shall have the authority to comply with Lawful U.S. Process and be given the corporate resources and authority to ensure such compliance and obtain the necessary support and participation of relevant employees of the Telkom Parties to that end.
- 2.5 **Network and Telecommunications Architecture:** Within **one hundred twenty (120) days** of the Effective Date, the Telkom Parties shall submit to the DOJ a comprehensive description of the DCI network(s), to include detailed transport network diagrams, and which may include a notice of whether any portion of the DCI is administered, maintained, operated, or owned by PT Telkom or Telin.
- (a) Thereafter, upon the DOJ's request, the Telkom Parties shall submit updated comprehensive descriptions of their DCI network(s), which may include an articulation of whether any portion of the DCI is administered, maintained, operated, or owned by PT Telkom or Telin.
 - (b) The submitted descriptions/diagrams shall include the 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. The comprehensive description also shall include the following information regarding the points of presence, NOCs, colocations, and peering points for the DCI:
 - 1) a description of the plans, processes, and/or procedures relating to network management operations that prevent the DCI and DC from being Accessed or controlled from outside the United States;
 - 2) a description of the placement of NOCs, data centers, and OSS hosting centers that support the DCI or DC;
 - 3) a description of any Telkom USA IP and broadband networks that are part of the DCI 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;

- 4) a description of any unique or proprietary application, platform, and or capability that supports the operation of the DCI and/or DC.

2.6 **Information Storage and Access:** The Telkom Parties shall make the following available in the United States:

- (a) stored DC, provided that such communications are otherwise stored by or on behalf of PT Telkom, Telin, or Telkom USA for any reason;
- (b) any Wire Communications or Electronic Communications (including any other type of wire, voice, or electronic communication not covered by the definitions herein of Wire Communication or Electronic Communication) that:
 - 1) are:
 - a. received by, intended to be received by, or stored in the account of a PT Telkom, Telin, or Telkom USA user or
 - b. routed to a PT Telkom, Telin, Telkom USA U.S. user, or routed to an PT Telkom, Telin, U.S. POP; and
 - 2) are otherwise stored by or on behalf of PT Telkom, Telin, or Telkom USA for any reason;
- (c) Transactional Data and Call Associated Data relating to DC if such information is otherwise stored by or on behalf of PT Telkom, Telin, or Telkom USA for any reason;
- (d) billing records relating to: (1) PT Telkom, Telin, or Telkom USA customers or subscribers for their U.S. operation, (2) PT Telkom, Telin, or Telkom USA customers and subscribers domiciled in the United States, (3) PT Telkom, Telin, or Telkom USA customers and subscribers who represent themselves to PT Telkom, Telin, or Telkom USA as being domiciled in the United States, and (4) any call routed through a PT Telkom, Telin, U.S. POP, provided that such billing-record information is otherwise stored by or on behalf of PT Telkom, Telin, or Telkom USA for any reason, 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, this Agreement, and the Implementation Plan;
- (e) Subscriber Information concerning: (1) PT Telkom, Telin, or Telkom USA customers or subscribers for those companies' U.S. operations, including information regarding telecommunications, broadband, wireless, broadcasts, Internet, wireline, video/programming in the United States, (2) PT Telkom, Telin,

or Telkom USA customers or subscribers who hold themselves out as being domiciled in the United States, and (3) related to any call routed through a PT Telkom, Telin, U.S. POP provided that such Subscriber Information is otherwise stored by or on behalf of PT Telkom, Telin, or Telkom USA for any reason;

- (f) a description of the placement of NOCs, data centers, and OSS hosting centers;
- (g) a description of PT Telkom, Telin's, and Telkom USA's IP/broadband networks located in the United States, if any, or supporting the DCI, or that are used for Telkom USA's DC processes 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 telecommunications service providers;
- (h) a description of any unique or proprietary control mechanisms of Telkom USA as well as of Telkom USA's operating and administrative software/platforms used for Telkom USA's provision of DC.

2.7 **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 within the United States to preserve any of the information enumerated in Section 2.6 herein, or upon receiving any other preservation request served in compliance with U.S. law, PT Telkom, Telin, or Telkom USA shall store such preserved records or other evidence in the United States in the manner and for so long as required by U.S. law.

2.8 **Mandatory Destruction**: The Telkom Parties shall ensure that the data and communications described in Section 2.6 of this Agreement are stored in a manner not subject to mandatory destruction under any foreign laws. The Telkom Parties shall further ensure that the data and communications described in Section 2.6 of this Agreement shall not be stored by or on behalf of PT Telkom, Telin, or Telkom USA solely outside of the United States.

2.9 **Billing Records**: PT Telkom, Telin, or Telkom USA shall store for at least **eighteen (18) months** post-bill generation all CDRs, CPNI, and other billing records generated that relate to DC and broadband services.

2.10 **Compliance with U.S. Law**: Nothing in this Agreement or the Implementation Plan shall excuse PT Telkom, Telin, or Telkom USA from any obligations they may have to comply with U.S. legal requirements for the retention, preservation, or production of information or data.

ARTICLE III

NON-OBJECTION BY THE GOVERNMENT PARTIES

- 3.1 **Non-Objection to Current Application:** Upon the execution of this Agreement by all of the Parties, the DOJ shall promptly notify the FCC that, provided the FCC conditions the grant of the FCC Application on PT Telkom's, Telin's, and Telkom USA's compliance with this Agreement, the DOJ has no objection to the FCC's grant or approval of the FCC Application. This assurance is given with the understanding that the Telkom Parties will submit the Implementation Plan as provided for herein and address any concerns raised by the DOJ with respect to the content and manifestation of, and compliance with, such Implementation Plan in a timely manner.
- 3.2 **Future Applications:** Nothing in this Agreement or the Implementation Plan shall preclude the DOJ from opposing, formally or informally, any FCC application by PT Telkom, Telin, or Telkom USA to transfer an FCC license to a third party or for other authority. The DOJ reserves the right 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 applications or petitions for such transfer or for other authority.

ARTICLE IV

SECURITY AND SECURE FACILITY

- 4.1 **Location of Secure Facility:** The Telkom Parties will maintain appropriately secure facilities (*e.g.*, offices, communications centers, NOCs, etc.) within the United States within which the Telkom Parties shall:
- (a) take appropriate measures to prevent unauthorized Access to data or facilities that might contain Classified Information or Sensitive Information, to include the development of appropriate visitation policies regarding visits to the DCI by foreign persons other than employees of Telkom USA;
 - (b) solely assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or that regularly deal with information identifiable to such U.S. citizens as Sensitive Information;
 - 1) If, after the Effective Date, PT Telkom, Telin, or Telkom USA deems it necessary to assign a non-U.S. citizen to a position referenced in Section 4.1(b), such party shall seek a waiver from Section 4.1(b)'s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-citizen candidate, and an explanation as to why such a waiver is necessary, to the DOJ. Any such waiver request must be submitted to the DOJ at least **thirty (30)** days prior to the desired date of any assignment of a non-U.S. citizen to any position falling within those outlined in Section 4.1(b). The

DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.1(b)1) to object to such request; *provided, however,* that if no objection is made by the DOJ within such thirty (30) day objection period, the waiver request shall be deemed approved by the DOJ. Should the DOJ, within its thirty (30) day objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and PT Telkom, Telin, or Telkom USA shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.1(b)1), the DOJ's thirty (30) day objection period shall be extended by the number of days the DOJ awaited a response from PT Telkom, Telin, or Telkom USA after the Telkom Party received the DOJ objection.

2) Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.1(b) pursuant to Section 4.1(b)1), the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated pursuant to Section 4.1(b)1) and submitted to the DOJ in the Annual Report required by Section 5.10. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.1(b)1), should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.1(b) unless another waiver is obtained pursuant to this Section 4.1(b) 1).

- (c) upon the DOJ's request, provide to the DOJ the PII of each person who regularly handles or deals with Sensitive Information;
- (d) require that personnel handling Classified Information, if any, shall be eligible for and possess appropriate security clearances prior to handling such information;
- (e) provide that the points of contact described in Section 4.5 shall have sufficient authority over any of PT Telkom's, Telin's, or Telkom USA's employees, if any, who may handle Classified Information or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority, and the terms of this Agreement and the Implementation Plan; and
- (f) handle and store any Sensitive Information and Classified Information, if any.

4.2 **Measures to Prevent Improper Use or Access:** The Telkom Parties shall take all reasonable security measures to prevent the use of or Access to the equipment or facilities supporting those portions of the DCI necessary for conducting Electronic Surveillance where such use or Access would violate any U.S. law or the terms of this Agreement or the Implementation Plan. These measures shall include technical, organizational,

personnel-related policies and written procedures, as well as necessary implementation plans and physical security measures.

4.3 **Access by Foreign Government Authorities:** Without the prior express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States, the Telkom Parties shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to, DC, Call Associated Data, Transactional Data, or Subscriber Information if such information is stored in the United States to any person if the purpose of such disclosure or Access is to respond to the legal process or the request of or on behalf of a foreign government, identified representative, or a component or subdivision thereof. Any such requests or submissions of legal process described in this Section 4.3 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 PT Telkom, Telin and Telkom USA, 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. PT Telkom, Telin and Telkom USA shall take reasonable measures to ensure that mechanisms are in place to become aware of all such requests or submission of legal process described in this Section 4.3.

4.4 **Disclosure to Foreign Government Authorities:** With respect to DC, the Telkom Parties shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

- (a) Classified Information or Sensitive Information, or
- (b) Subscriber Information, Transactional Data, Call Associated Data, or a copy of any Wire Communication or Electronic Communication, intercepted or acquired pursuant to Lawful U.S. Process

to any foreign government, identified representative, or a component or subdivision thereof without satisfying all applicable U.S. federal, state, and local legal requirements pertinent thereto, and without obtaining the prior express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. The Telkom Parties shall notify the DOJ of any requests or any legal process submitted to PT Telkom, Telin, or Telkom USA by a foreign government, identified representative, or a component or subdivision thereof for communications, data, or information identified in this Section 4.4. The Telkom Parties shall provide such notice 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 PT Telkom, Telin, or Telkom USA, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. The Telkom Parties shall take reasonable measures to ensure that they will promptly learn of all such requests or submission of legal process described in this Section 4.4.

- 4.5 **Law Enforcement Point of Contact (“LE POC”)**: Within **forty-five (45) days** after the Effective Date, Telkom USA shall designate a LE POC within the United States with the authority and responsibility for accepting and overseeing compliance with Lawful U.S. Process. Within that same period of time, Telkom USA shall notify the DOJ of the designation of the LE POC, and include in such notice the PII for the LE POC.
- (a) Thereafter, Telkom USA shall notify the DOJ of any change in the designation(s) for LE POC within **ten (10) business days** of such change. Any notice of a new LE POC shall include the PII for the newly designated individual.
 - (b) The LE POC shall be resident U.S. citizens who are eligible for appropriate U.S. security clearances. Telkom USA shall cooperate with any request by a government entity within the U.S. regarding a designated LE POC’s availability for a background check and/or a security clearance process.
 - (c) The LE POC will be required to 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:
 - 1) Sensitive and Classified Information, if any;
 - 2) any Lawful U.S. Process for Electronic Surveillance, and the information pertaining thereto, including the content of the results from executing the Lawful U.S. Process, in accordance with the requirements of U.S. law.
- 4.6 **Security of Lawful U.S. Process, Sensitive Information, and Classified Information**: The Telkom Parties shall protect the confidentiality and security of all Lawful U.S. Process served upon them, and the confidentiality and security of Classified Information, if any, and Sensitive Information in accordance with U.S. federal and state law or regulations.
- 4.7 **Change in Service Portfolio**: The Telkom Parties will inform the DOJ at least **ninety (90) days in advance** of any material changes to the current-services portfolio for Telkom USA or any successor in interest to Telkom USA, and of offers of other services beyond such portfolio, including the commencement of the provision of facilities-based DC not previously notified to the DOJ.
- (a) The Parties enter into this Agreement with the understanding that, as of the Effective Date, such portfolio is no different from that submitted by Telkom USA in its Team Telecom responses electronically received by the DOJ on December 23, 2015. In short, such understanding is that Telkom USA’s intentions as of the Effective Date are to provide wholesale transport between the U.S. and Indonesia to third-party carrier customers and transport to enterprise-level customers; and that Telkom USA does not intend to provide retail services to other types of customers.

- 4.8 **Access to Classified or Sensitive Information:** Nothing contained in this Agreement or the Implementation Plan shall limit or affect the authority of a Government Authority within the United States, under that agency's jurisdiction, to grant, deny, modify, or revoke PT Telkom, Telin's, or Telkom USA's Access to Classified and Sensitive Information.
- 4.9 **Designation of Security Officer and/or Technical Compliance Officer ("SOTCO" or "Security Officer"):** The Telkom Parties must designate and maintain a SOTCO for purposes of this Agreement. The SOTCO will have the appropriate authority and skills to implement the terms of this Agreement and to address security concerns identified by the DOJ touching upon compliance with this NSA. The SOTCO shall have the appropriate senior-level corporate authority within Telkom USA to perform his/her duties under this Agreement and the Implementation Plan. The SOTCO also shall possess the necessary authority, resources and skills to ensure compliance with this Agreement and to act as a liaison to the DOJ regarding the Telkom Parties' compliance with the NSA and the Implementation Plan and to address any national security issues arising in Telkom USA's due course of business. The Telkom Parties shall need to provide the SOTCO with Access to that business information of the Telkom Parties that is necessary for the SOTCO to perform his or her duties.
- (a) The Telkom Parties shall designate their initial SOTCO to the DOJ within **seventy-five (75) days** of the Effective Date, and thereafter shall provide at least **fourteen (14) days'** notice of a SOTCO's departure, and **thirty (30) days' prior notice** of a new SOTCO designation. The Telkom Parties shall not maintain a vacancy or suspension of the SOTCO position for a period of more than **sixty (60) days** unless DOJ objects to a designee noticed in a timely manner, in which case the sixty-day period is extended for the length of time the DOJ took to object to a designee.
- (b) All SOTCO designations shall be subject to DOJ review and non-objection, and the Telkom Parties shall reasonably address any concerns raised by the DOJ regarding the selection and identity of the SOTCO. The DOJ shall make its objections to a new SOTCO designee within **forty-five (45) days** after receiving notice.
- (c) With respect to any SOTCO, he/she must:
- 1) be a resident U.S. citizen who possesses U.S. citizenship only (i.e., is not a dual-national);
 - 2) if not already in possession of a U.S. security clearance, shall be eligible, at the sole discretion of the USG, to hold such security clearances following appointment;
 - 3) be subject to the screening process described in Sections 4.13 and 4.14;

- 4) reside in the continental U.S., in a location that permits and supports the SOTCO's efficient and successful fulfillment of his duties and obligations under the NSA and the Implementation Plan; and
- 5) be a corporate officer with appropriate authority, skills, and resources to ensure compliance with this Agreement.

For the avoidance of doubt, the Telkom Parties may designate a single SOTCO that meets the above criteria but, in lieu of subsection 5) above, is a corporate officer of Telkom USA with appropriate authority, skills, and resources to ensure compliance by Telkom USA with this Agreement and additionally has been granted by PT Telkom and Telin the appropriate corporate authority, skills, resources, and support to ensure compliance by PT Telkom and Telin with their respective obligations under this Agreement.

4.10 **SOTCO Responsibilities and Duties:** The responsibilities and duties of the SOTCO shall include, at least, each of the following:

- (a) Providing the DOJ the Annual Report required under Section 5.10 of this Agreement;
- (b) Developing and maintaining the Implementation Plan, along with Telkom USA's Information Security Plan (Section 4.11), Access-or-disclosure requirements (described in Sections 4.2, 4.3, and 4.4), Offshoring Control and Access Policy (Section 4.12), personnel-screening-process requirements (described in Sections 4.13 and 4.14), and other policies generally discussed herein (*e.g.*, regarding visitation (Section 4.1(a)) and trade secrets protection (Section 4.15), etc.) 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 interim reports to the DOJ mandated by this Agreement;
- (e) Being aware of, and reporting to the DOJ, 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 DOJ relating to the enforcement of and compliance with the Agreement or any other issue involving national security;
- (g) Ensuring procedures are in place for the Telkom Parties to comply with Lawful U.S. Process in an expeditious, effective, and unimpeded fashion; and

(h) Acting as the liaison with and point of contact for the Telkom Parties for the DOJ.

4.11 **Information Security Plan:** Following the Effective Date, the Telkom Parties shall create, amend, maintain, or adapt an information security plan that, as further expanded upon and explained in the Implementation Plan, at the very least:

(a) Takes appropriate measures to prevent unauthorized Access to DC and DCI and/or facilities that might contain Classified or Sensitive Information;

(b) Ensures assignment of U.S. citizens to positions for which screening is contemplated pursuant to Section 4.13(a);

- 1) If, after the Effective Date, PT Telkom, Telin, or Telkom USA deem it necessary to assign a non-U.S. citizen to a position referenced in Section 4.11(b), such party shall seek a waiver from Section 4.11(b)'s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-citizen candidate, and an explanation as to why such a waiver is necessary, to the DOJ. Any such waiver request must be submitted to the DOJ at least **forty-five (45)** days prior to any assignment of a non-U.S. citizen to any position falling within those outlined in Section 4.11(b). The DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.11(b)1) to object to such request; *provided, however*, that if no objection is made by the DOJ within such thirty (30)-day-objection period, the waiver request shall be deemed approved by the DOJ. Should the DOJ, within its thirty (30)-day-objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and PT Telkom, Telin, or Telkom USA shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.11(b) 1), the DOJ's thirty (30)-day-objection period shall be extended by the number of days the DOJ awaited a response from PT Telkom, Telin, or Telkom USA after the Telkom Party received the DOJ objection.
- 2) Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.11(b) pursuant to Section 4.11(b)1), the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated and submitted to the DOJ in the Annual Report required by Section 5.10. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.11(b)1), should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.11(b) unless another waiver is obtained pursuant to this Section 4.11(b)1).

- (c) Assigns 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 persons as Sensitive Information;
- (d) Specifies that, upon request from the DOJ, PT Telkom, Telin, and/or Telkom USA shall provide to the DOJ the PII and other relevant requested identifier information of each person who regularly handles or deals with Sensitive Information;
- (e) Requires that personnel handling Classified Information shall have been granted appropriate security clearances, consistent with Executive Orders 12,968 and 13,467 and other applicable law;
- (f) Ensures that the LE POC described in Section 4.5 of this Agreement shall have sufficient authority over any employees or contractors of PT Telkom, Telin, or Telkom USA who may handle Classified Information or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;
- (g) Ensures that the disclosure of or Access to Classified Information or Sensitive Information is limited to those who have appropriate security clearances and authority consistent with Executive Orders 12,968 and 13,467 and other applicable law;
- (h) Identifies 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 the Telkom Parties will accept or reject Screened Personnel (as defined in Section 4.13);
- (i) Maintains appropriately secure facilities (*e.g.*, offices, communications centers, network operations centers, etc.) within the U.S. for the handling and storage of any Classified Information or Sensitive Information; and
- (j) Ensures only appropriate personnel may Access non-public information regarding internal Telkom USA personnel, contractors, service partners, subscribers, or users.

4.12 **Outsourcing and Offshoring Control and Access:**

- (a) The Telkom Parties shall not Outsource or Offshore functions covered by this Agreement to an entity that is not within the definition of “Telkom USA” under this Agreement, except pursuant to the Outsourcing and Offshoring Control and Access Policy adopted pursuant to this NSA and the Implementation Plan, as outlined in Section 4.12(b).

- 1) Where the Telkom Parties already are Outsourcing or Offshoring functions covered by this Agreement, such Outsourcing or Offshoring functions shall be considered exempt from this subsection's prohibition.
 - 2) In order to assess future compliance with Section 4.12(a), the Telkom Parties shall submit to the DOJ a notice of current Outsourcing/Offshoring providers of functions covered by this Agreement within **sixty (60) days** of the Effective Date.
- (b) No later than **one hundred twenty (120) days** after the Effective Date, the Telkom Parties will adopt and implement an Outsourcing and Offshoring Control and Access Policy. The Telkom Parties shall consult with the DOJ regarding the memorialization, design, and implementation of such policy, and shall reasonably address any concerns raised by the DOJ with respect to such memorialization, design, and implementation. Further, such policy shall require PT Telkom, Telin, and/or Telkom USA, as applicable, to provide the DOJ **sixty (60) days'** prior notice of any proposed Outsourcing or Offshoring, and the right of the DOJ to object within **forty-five (45) days** of receipt of such notice to the proposed Outsourcing or Offshoring.
- 1) All Outsourcing and Offshoring arrangements shall be subject to the Telkom Parties Outsourcing and Offshoring Control and Access Policy, which shall include logical and physical controls (such as restricted access methods and background screening).
 - 2) The Telkom Parties shall not Outsource or Offshore functions involving DCI (to the extent, that Telkom USA has and maintains DCI), DC, Access to Classified Information, Sensitive Information, or Lawful U.S. Process; and the Telkom Parties' Outsourcing and Offshoring Control and Access Policy may not provide for such outsourcing/offshoring.
 - 3) The Outsourcing and Offshoring Control and Access Policy may address classes of Outsourcing or Offshoring contracts of a routine and nonsensitive nature to be excluded from Section 4.12(b)'s notice-and-approval requirement.

4.13 **Screening of Personnel:** The Telkom Parties shall maintain and implement a screening process to ensure compliance with all personnel-screening-process requirements agreed to herein and in the Implementation Policy. The screening process of the Telkom Parties shall cover any existing or newly hired employees and any personnel performing under an agreement with PT Telkom, Telin, or Telkom USA requiring Access/responsibilities in at least the following circumstances:

- (a) All persons who have Access to Classified or Sensitive Information; all persons who have Access to DCI to monitor the content of DC; and all persons who have the ability to monitor personnel with limited access to DC under this subsection.

- (b) All persons who have Access to Transactional Data, Subscriber Information, CPNI, CDRs, IPDRs, or PII for customers and network users of Telkom USA; all persons who have limited access DCI excluding the ability to monitor the content of DC; and all persons who provision network elements either onsite or remotely.
- (c) Nothing in this subsection shall be read to apply the screening requirements in Section 4.13 to PT Telkom/Telin/Telkom USA 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, the Telkom Parties will cooperate with any reasonable notice by the DOJ to provide additional information necessary for an enhanced background investigation to be conducted by such DOJ with respect to identified Screened Personnel.

4.14 **Screening Process Requirements:** The screening process undertaken pursuant to Sections 4.13 and 4.14 of this Agreement shall be implemented through a reputable third party, and shall specifically include a background check in addition to a criminal records’ check. The Telkom Parties shall consult with the DOJ on the screening procedures utilized by the reputable third party and shall provide to the DOJ a list of the positions subject to screening no later than **one hundred fifty (150) days** after the Effective Date. Thereafter, the Telkom Parties shall notify the DOJ of changes to the list of positions subjected to screening (*i.e.*, either adding to or removing classes of positions) within **sixty (60) days** of such change.

- (a) The Telkom Parties shall utilize the criteria identified pursuant to Section 4.13 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 DOJ all the information collected through the 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 DOJ, and the candidates shall consent to the sharing of this information with the DOJ. In addition:

- 1) The Telkom Parties shall assign U.S. citizens to positions for which screening is contemplated pursuant to Section 4.13(a).
 - a. If, after the Effective Date, PT Telkom, Telin, or Telkom USA deems it necessary to assign a non-U.S. citizen to a position referenced in Section 4.14(a)1), such party shall seek a waiver from Section 4.14(a)1)’s U.S.-citizenship requirement by sending the PII of the relevant non-U.S.-citizen candidate, and an explanation as to why such a waiver is necessary, to the DOJ. Any such waiver request must be submitted to the DOJ at least **forty-five (45) days** prior to any assignment of a non-U.S. citizen to any position falling within those outlined in Section 4.14(a)1). The

DOJ shall have **thirty (30) days** following receipt of any waiver request made pursuant to this Section 4.14(a)1)a. to object to such request; *provided, however*, that if no objection is made by the DOJ within such thirty (30) day objection period, the waiver request shall be deemed approved by the DOJ. Should the DOJ, within its thirty (30) day objection period, seek additional information regarding a waiver request or the non-U.S.-citizen candidate at issue, the DOJ shall make every effort to ensure that such inquiry is reasonable, and PT Telkom, Telin, or Telkom USA shall promptly respond to such inquiry. In the event that the DOJ seeks additional information regarding a waiver request pursuant to this Section 4.14(a)1)a., the DOJ's thirty (30) day objection period shall be extended by the number of days the DOJ awaited a response from PT Telkom, Telin, or Telkom USA after the Telkom Party received the DOJ inquiry.

- b. Should the DOJ grant a request to waive the U.S.-citizenship requirement of Section 4.14(a)1) pursuant to Section 4.14(a)1)a., the name(s) of the non-U.S.-citizen candidate(s) at issue in that waiver shall be added to the list of persons routinely updated and submitted to the DOJ in the Annual Report required by Section 5.10. Once a non-U.S. citizen is the subject of a waiver pursuant to Section 4.14(a)1)a., should such person leave his/her position, such person's replacement must comport with the U.S.-citizen requirements of Section 4.14(a)1) unless another waiver is obtained pursuant to this Section 4.14(a)(1)(a).
- 2) The Telkom Parties may Outsource or Offshore positions for which screening is contemplated pursuant to Section 4.13(b).
 - a. With respect to Outsourced or Offshored personnel, the Telkom Parties shall ensure that such personnel are subject to restricted Access methods and background screening requirements under the terms of the Outsourcing and Offshoring Control and Access Policy, in accordance with Section 4.12 of this Agreement.
- 3) The Telkom Parties shall consult with the DOJ regarding the screening procedures to be used and the positions subject to screening. The Telkom Parties shall reasonably address any concerns the DOJ may raise with respect to such screening procedures. The Telkom Parties shall use the criteria identified in Section 4.13 of this Agreement to identify the personnel to be screened.
- 4) The Telkom Parties shall cooperate with reasonable requests by the DOJ, or any USG Authority, desiring to conduct any further background checks

for persons falling within the screening requirements of Sections 4.13 and 4.14.

- a. Individuals who are rejected pursuant to such further background checks by the DOJ or a USG Authority shall not be permitted to perform functions that would require screening under this Agreement.
- 5) The Telkom Parties shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.
- 6) The Telkom Parties shall maintain records relating to the status of Screened Personnel, and shall provide such records, upon request, to the DOJ.
- (b) Any records or other information relating to individual persons provided to or obtained by the DOJ in connection with this Agreement, including implementation and results of Screening Requirements outlined in Section 4.14 of this NSA, shall be maintained in a secure and confidential manner strictly in accordance with applicable law.

4.15 **Protection of Trade Secrets:** Telkom USA shall affirmatively behave in manners, ways, and means that will demonstrate its desires to protect and maintain the confidentiality of the trade-secret and proprietary information in its businesses possession(s) to the extent that the safeguarding of such information is necessary to protect Classified Information, Sensitive Information, Subscriber Information, DC, DCI, Call Associated Data, CPNI, Transactional Data, and customer PII, related to Telkom USA's provision of DC, from inadvertent, unintended, or improper disclosure, or is otherwise relevant to carrying out the provisions of this NSA.

- (a) Within **one hundred and twenty (120)** days of the Implementation Plan's Adoption Date, Telkom USA shall undertake an internal review to determine, in its reasonable discretion, what, if any, Trade Secrets or other proprietary information it possesses related to Telkom USA's provision of DC. Thereafter, Telkom USA shall engage in periodic internal reviews to confirm it is adequately identifying Trade Secret and proprietary information related to Telkom USA's provision of DC. Such periodic internal reviews shall occur at reasonable intervals for doing so, with no more than **three (3) years** passing between each internal review.
- (b) Should Telkom USA, through conducting an internal review of the type described in this Section 4.15(a), identify any Trade Secrets or proprietary information, related to Telkom USA's provision of DC, it shall:

- 1) Evaluate the risks to their business(es) presented by the potential for third party unauthorized access to such Trade Secrets or proprietary information; and
- 2) Take those steps they deem appropriate to mitigate such risks.

ARTICLE V

AUDITING, REPORTING AND NOTICE

- 5.1 **Notice of Obligations:** The Telkom Parties shall instruct appropriate officials, employees, contractors and agents as to the Telkom Parties' obligations under this Agreement and the Telkom Parties' obligations under the Implementation Plan that the officials, employees, contractors and agents will assist the Telkom Parties to comply with, and issue periodic reminders of such obligations to such persons. Records of such instructions shall be maintained by the Security Officer.
- 5.2 **Reporting of Incidents:** The Telkom Parties shall take all practicable steps under the Implementation Plan to ensure that they shall notify the DOJ if any PT Telkom, Telin, or Telkom USA official, employee, contractor, or agent, respectively, acquires any information that reasonably indicates the following occurred:
- (a) a breach of this Agreement or the Implementation Plan;
 - (b) unauthorized or improper Access to or disclosure of DC, or the unauthorized or improper conduct of Electronic Surveillance carried out in violation of U.S. law;
 - (c) Access to or disclosure of CPNI or Subscriber Information in violation of U.S. federal, state or local law or regulation (except for violations of FCC regulations relating to improper use of CPNI); or
 - (d) improper Access to or disclosure of Classified Information or Sensitive Information.

PT Telkom, Telin's and Telkom USA's notification shall be made promptly and in any event no later than **ten (10) calendar days** after PT Telkom, Telin, or Telkom USA management acquires such information. Further, the Telkom Parties shall lawfully cooperate in investigating the matters pertaining to such notice. The Telkom Parties need not report information where its disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

- 5.3 **Notice of Decision to Store Information Outside the United States:** As of the Effective Date, the Telkom Parties have no plans to store DC, Transactional Data, Call Associated Data, Subscriber Information, CDRs, CPNI, or other billing records of the types identified in Section 2.6(d) or that otherwise relate to DC outside of the U.S. or enter into contracts or other arrangements for such storage. Telkom USA shall provide

the DOJ with **forty-five (45) days'** prior written notice regarding the storage outside of the U.S. by PT Telkom, Telin, Telkom USA, or any entity with which PT Telkom, Telin, or Telkom USA have contracted or made other arrangements for data or communications processing or storage of DC, Transactional Data, Call Associated Data, Subscriber Information, CDRs, CPNI, or other billing records of the types identified in Section 2.6(d) or that otherwise relate to DC. Such notice shall, at a minimum:

- (a) include a description of the type of information to be stored outside the United States;
- (b) identify the custodian of the information (even if such custodian is PT Telkom, Telin, or Telkom USA);
- (c) identify the location where the information is to be stored; and
- (d) identify the factors considered in deciding to store the information outside of the United States.

The DOJ shall have **thirty (30) days** to object to the notified storage arrangement, with such objection having the effect of terminating such plans. The DOJ's failure to object within such thirty (30) day period shall be considered equivalent to a non-objection of the notified storage arrangement.

5.4 **Notice of Decision to Use Foreign-Located Communication Infrastructure:** The Telkom Parties shall provide the DOJ **sixty (60) days'** advance written notice if PT Telkom, Telin, or Telkom USA plan to provide, direct, control, supervise, or manage DC through any facilities located outside of the United States and its territories. Upon receipt of such a notice, the DOJ shall have **forty-five (45) days** to provide an objection to PT Telkom, Telin, or Telkom USA's notified plans. Such notice from PT Telkom, Telin or Telkom USA shall, at a minimum:

- (a) include a description of the facilities to be located outside the United States, and a description of the functions of the facilities;
- (b) identify the location where the facilities are to be;
- (c) identify the factors considered in making the decision; and
- (d) identify the security provisions taken by the Telkom Parties to protect DC and DCI.

The DOJ's failure to notify Telkom USA of any objection within such forty-five (45) day period shall be considered equivalent to a non-objection of the notified plans.

5.5 **Outsourcing Third Parties:** If PT Telkom, Telin, or Telkom USA outsources to third parties any function covered by this Agreement or the Implementation Plan, PT Telkom,

Telin, and/or Telkom USA, respectively, shall take reasonable steps to ensure that those third parties comply with the applicable terms of this Agreement and Implementation Plan; and, the Telkom Parties' Outsourcing and Offshoring Control and Access Policy (as contemplated by Section 4.12 of this NSA) shall memorialize this requirement. The reasonable steps that must be taken shall include:

- (a) inserting in the contracts of such third parties, executed on or after the Effective Date (including, for the avoidance of doubt, the subsequent renewal or extension of any contracts with outsourcing third parties with which PT Telkom, Telin, and/or Telkom USA have a contract as of the Effective Date), written provisions requiring that such third parties comply with all applicable terms of the Agreement and Implementation Plan; and
- (b) taking other reasonable, good-faith measures to ensure that such third parties are aware of, agree to comply with, and are bound by the applicable obligations under this Agreement and Implementation Plan (*e.g.*, providing copies of and training regarding the Agreement and Implementation Plan to such third parties, and requiring acknowledgement forms with respect to their obligations from such third parties, etc.).

If PT Telkom, Telin, or Telkom USA learn that an outsourcing third party or the outsourcing third party's employee has violated a provision of this Agreement or the Implementation Plan, PT Telkom, Telin, or Telkom USA, shall notify the DOJ as promptly as possible, and, in any event, no later than **three (3) calendar days** after the Telkom Party learns of the violation. Following such notification, and in consultation with the DOJ, the Telkom Parties will take the steps necessary to rectify the situation as soon as reasonably practicable, which steps may include, among others, terminating the arrangement with the outsourcing third party, initiating and pursuing litigation or other remedies at law and/or equity, and/or assisting and cooperating with the DOJ in pursuing legal and/or equitable remedies.

5.6 **Access to Information:** In response to reasonable requests made by the DOJ, the Telkom Parties shall provide the DOJ with Access to information concerning technical, physical, management, or other security measures and other reasonably available information related to the Telkom Parties' compliance with the terms of this Agreement and the Implementation Plan.

5.7 **DOJ Visits and Inspections:** Upon reasonable notice and during reasonable business hours, the DOJ may visit and inspect any part of PT Telkom's, Telin's and Telkom USA's DCI, secure facilities, corporate offices in the United States, and such other facilities that the parties and DOJ may agree upon in writing are relevant to this Agreement for the purpose of verifying compliance with the terms of this Agreement and the Implementation Plan. The Telkom Parties may have appropriate PT Telkom, Telin, or Telkom USA employees accompany DOJ representatives throughout any such inspection.

- 5.8 **DOJ Access to Personnel:** Upon reasonable notice from the DOJ, the Telkom Parties will make available for interview officers or employees of the Telkom Parties that are located in the United States and in a position to provide information to verify compliance with this Agreement and will seek to require contractors supporting the provision of DC or the compliance with this Agreement or the Implementation Plan to make available appropriate personnel that are located in the United States and are in a position to provide information to verify compliance with this Agreement and the Implementation Plan.
- 5.9 **Approval of Managed Network Service and Principal Equipment Providers:** No later than **forty-five (45) days** after the Effective Date, the Telkom Parties shall provide the DOJ with a list of names of all Managed Network Service Providers and Principal Equipment providers supporting the DCI and DC, including entities that perform any maintenance, repair, or replacement of the DCI that could result in any material modification to the Principal Equipment or systems or software used with or supporting the Principal Equipment. Such list shall not only identify the Managed Network Service Provider(s) or Principal Equipment, respectively, but also identify the manner/type of service or type of equipment offered by such Managed Network Service Provider(s) or Principal Equipment Provider(s).
- (a) PT Telkom, Telin, and/or Telkom USA shall notify the DOJ at least **sixty (60) days** before using any Managed Network Service Provider or Principal Equipment Provider supporting the DCI or DC not previously identified to the DOJ or where there will be changes in the service offerings/support from already identified Managed Network Service Providers and Principal Equipment Providers (i.e., where an already identified provider will be offering support in a previously unidentified way). The DOJ shall have **forty-five (45) days** to object, unless otherwise delayed by awaiting responses to inquiries for further information from the Telkom Parties, in which event the DOJ shall be afforded additional time to approve or disapprove any request sent to the DOJ under this Section 5.9. The DOJ's additional time to approve or disapprove such request shall be either the original **forty-five (45)-day** window extended by the number of days the DOJ awaited a response from PT Telkom, Telin, and/or Telkom USA after the inquiry is received by Telkom USA or **fourteen (14) days** after a response from PT Telkom, Telin, and/or Telkom USA is received, whichever is greater. Should the DOJ object, the notified Managed Network Service Provider and/or Principal Equipment Provider shall not be utilized for the notified purpose. Failure by the DOJ to object, within the original 45-day window, including any extension provided for in this subsection, or within 14 days after receiving a response from PT Telkom, Telin, or Telkom USA, whichever is greater, shall be deemed to constitute a non-objection to the requested use of such Managed Network Service Provider(s) or Principal Equipment Provider(s).
- (b) In the event of an emergency, as reasonably determined by the SOTCO, such as an instance requiring immediate maintenance or repair of facilities and use of a service or equipment for which the necessary Managed Network Service Provider

or Principal Equipment Provider has not already been notified to the DOJ, PT Telkom, Telin, or Telkom USA may utilize the provider or supplier, provided that PT Telkom, Telin, or Telkom USA provide notice to the DOJ as promptly as practicable, and in no event longer than **three (3) business days** after the initial use of such provider. PT Telkom, Telin, or Telkom USA may continue to utilize the provider, provided that the DOJ does not object within **forty-five (45) days** of notification to the DOJ, or within the additional time necessary for PT Telkom, Telin, and/or Telkom USA to answer DOJ questions, as outlined for the process in Section 5.9.

- (c) The emergency authority conferred in Section 5.9(b) may be suspended at will by the DOJ for any length of time deemed necessary by the DOJ should it conclude in a particular exercise of that authority either that the SOTCO did not reasonably determine that there was an emergency under Section 5.9(b) or that PT Telkom, Telin, and/or Telkom USA, or the SOTCO, did not follow the applicable procedures of Section 5.9(b). Such suspension by the DOJ must be in writing, and can only be rescinded thereafter by the DOJ in writing or by order of a court of competent jurisdiction hereunder. The DOJ shall reasonably and promptly engage with PT Telkom, Telin, and/or Telkom USA regarding any suspension of Section 5.9(b) under this Section 5.9(c).

5.10 **Annual Report:** On or before the yearly anniversary of the Effective Date, the SOTCO shall submit to the DOJ a report assessing PT Telkom, Telin's, and Telkom USA's compliance with the terms of this Agreement and the Implementation Plan for the preceding twelve-month period. The report shall at a minimum include:

- (a) a list of all of the active policies and procedures adopted to comply with this Agreement and the Implementation Plan, along with each document's date of adoption;
- (b) a copy of the policies and procedures adopted in the reporting year to comply with this Agreement and the Implementation Plan, if any;⁴
- (c) a summary of the changes, if any, to such policies and procedures, and the reasons for those changes;
- (d) a summary of known acts of non-compliance with the terms of this Agreement and the Implementation Plan, whether inadvertent or intentional, if any, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future;

⁴ PT Telkom, Telin, and/or Telin USA agree, however, to provide the DOJ with copies of any active policies adopted in prior years upon request.

- (e) an identification of other issues, if any, that could affect the effectiveness of or compliance with this Agreement or the Implementation Plan;
- (f) a list of all of the notices submitted to the DOJ during the prior year, if any;
- (g) a current list of all Managed Network Service Providers and Principal Equipment Providers, if any, including the manner/type of support from each;
- (h) updated network security policies and implementation procedures, if any;
- (i) an identification of any material information with respect to this Agreement not specifically identified in this Section 5.10;
- (j) an identification of material cybersecurity incidents, in accordance with the Implementation Plan, to include material malicious and persistent network attacks, enterprise intrusions/unauthorized Access, viruses, phishing electronic-mail (“e-mail”) messages, penetrative network interference, unauthorized network shut-downs, and/or similar threats; and
- (k) a list of all non-U.S. citizen personnel who, as of the date of the Annual Report, either remain working in the positions and/or capacities already notified to the DOJ pursuant to Sections 4.1(b)1), 4.11(b)1), and 4.14(a)1)a. of this NSA or who need to be added to the list pursuant to Sections 4.1(b)2), 4.11(b)2), and 4.14(a)1)b of this NSA.

5.11 **Third-Party Network Security Audits:** The Telkom Parties shall retain and pay for a neutral third party technical engineer or subject matter expert to objectively audit PT Telkom, Telin’s, and Telkom USA’s operations and compliance with this NSA every two years, provided that the DOJ may request that the Telkom Parties commission an audit during the interim year between standard audit reports should the need arise, as determined by the DOJ. Should the DOJ request an interim audit, the DOJ will tailor the scope of that audit to those areas of most interest to the DOJ.

- (a) The final audit report for the first audit commissioned under this section shall be due **fifteen (15) months** from the Implementation Plan’s Adoption Date, with the final reports for each subsequent audit due every **two (2) years** thereafter (*e.g.*, the second final audit report would be due **three (3) years and three (3) months** after the Implementation Plan’s Adoption Date; the third, five years and three months after; etc.) (each such subsequent audit referred to herein as a “Biennial Audit”). Should the DOJ request an interim audit, that request shall have no bearing on the due date for the audit otherwise due under this Section 5.11 at the end of the relevant two-year period between standard audits, unless otherwise waived by the DOJ.
- (b) The Telkom Parties shall provide notice within **eight (8) months** after the Implementation Plan’s Adoption Date of, and terms of reference for, their

selected auditor to the DOJ, and the DOJ shall have an opportunity to review and object to the selected auditor within **thirty (30) days** of receiving such notice. In the event of a DOJ objection to a selected auditor, the Telkom Parties shall work in good faith to resolve such objection and additional time for completion of the audit will be provided as may become reasonably necessary as a result of the time needed to resolve any DOJ objection. For the avoidance of doubt, the provision of any additional time for completion of the audit will not alter the due date of subsequent Biennial Audits. In the absence of any timely notice of DOJ objection, the selected auditor will be deemed approved.

- (c) The Telkom Parties shall provide to the DOJ a copy of the contract with the selected auditor, which shall include terms defining the scope and purpose of the audit. The DOJ shall have the right to review and comment on such terms, but such comments must be sent to the Telkom Parties within **forty-five (45) days** of the DOJ's receipt of such terms. In the event of the DOJ commenting on an audit's terms, the Telkom Parties shall work in good faith to resolve the DOJ's comments and request changes and/or insertions by the DOJ.
- (d) Through their contract with the selected auditor, the Telkom Parties shall ensure that all reports generated by the auditor are provided promptly to the DOJ.
- (e) At a minimum, the terms defining the scope and purpose of the initial audit and Biennial Audits thereafter shall include:
 - 1) Development of an initial vulnerability and risk assessment of Telkom USA's DC and DCI based on this Agreement, and a detailed audit work plan based on such assessment.
 - 2) Authority for the auditor to review and analyze the Telkom Parties' security policies and procedures related, as applicable, to the provision of DC and the DCI, methods for protecting the companies' trade secrets touching upon the matters addressed in this Agreement, and those policies discussed in this NSA;
 - 3) Authority to audit the integrity of password systems, review access logs, Syslogs, and review logs regarding any access to the DCI to a capacity to conduct Electronic Surveillance;
 - 4) Authority for the Auditor to review reports, summaries, and other information regarding PT Telkom, Telin's, and Telkom USA's efforts to monitor network devices via logs and active polls for unauthorized access or access above assigned privileges, including to U.S. Records, and to include any known security issues;

- 5) Authority for the auditor to conduct a reasonable number of unannounced inspections of PT Telkom, Telin's, and Telkom USA's facilities that support the Telkom Parties' obligations under this NSA; and
 - 6) Authority for the auditor to conduct a reasonable volume of random testing of network firewalls, access points, and other systems on the DCI for potential vulnerabilities.
- 5.12 **Network Changes**: PT Telkom, Telin, and/or Telkom USA will report to the DOJ any major-network provisions or upgrades and changes to Principal Equipment providers, Managed Network Service Providers, and third-party contractors supporting the DCI or functions related to compliance with the Telkom Parties' obligations under this Agreement, within **thirty (30) days** of such upgrades or changes being implemented, unless other manner of notice is specifically mandated herein (*e.g.*, Section 5.9).
- 5.13 **Change In Control of Telkom USA**: Telkom USA shall provide the DOJ written notice and copies of any filing(s) with the FCC or any other USG agency relating to the *de jure* or *de facto* change in control of Telkom USA, except for filings with the FCC for assignments or transfers of control that are *pro forma*. Telkom USA shall provide such notices and copies to the DOJ within **seven (7) business days** of the applicable filing date(s).
- 5.14 **Corporate Restructuring**: Telkom USA shall promptly notify the DOJ of any corporate restructuring that involves the insertion or removal of an entity or person having direct or indirect *de jure* or *de facto* ownership or control of Telkom USA.
- 5.15 **Notices**: All communications or other notices relating to this Agreement or the Implementation Plan, including any DOJ objections or replies in response to PT Telkom, Telin, or Telkom USA notices hereunder or Telkom Party responses to DOJ objections or notices, must be provided in writing and may be delivered in any manner and form discussed herein, to the individuals identified herein or to such persons notified to the Parties in the future as updated points of contact with respect to the NSA. All communications, objections, responses, or other notices relating to this Agreement or the Implementation Plan shall be deemed both given and received:
- (a) when delivered personally;
 - (b) if by e-mail, as of the electronic time stamp in the DOJ's e-mail account(s);
 - (c) if sent by documented overnight courier service, on the date delivered; or
 - (d) if sent by mail, five (5) business days after being mailed by registered or certified U.S. mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the Parties may designate in accordance with this Section.

The following contact information shall be used for each of the delivery methods specified in subsections (a) – (d) above:

For the DOJ:

U.S. Department of Justice
Assistant Attorney General for National Security
Attn: Director, Foreign Investment Review Staff
600 E St. NW, 10th Floor
Washington, DC 20004
E-mail: ttelecom@usdoj.gov

For PT Telkom:

Donny Kertaputra Widjaja
AVP Contract and Transaction
PT Telekomunikasi Indonesia Tbk
Jl. Japati No. 1
Bandung 40133 – Indonesia
Fax: +62 21 521 5432
E-mail: kertaputra@telkom.co.id

For Telin:

G.E. Dhany Widjajanta
VP Corporate Secretary
PT Telekomunikasi Indonesia International
Menara Jamsostek, North Tower 24th Floor
Jl. Jend. Gatot Subroto Kav.38
Jakarta 12710 – Indonesia
Fax: +62 21 5296 2358
E-mail: dhany@telin.co.id

For Telkom USA:

Joseph Sahat Raja
Chief Executive Officer
Telekomunikasi Indonesia International (USA) Inc.
800 Wiltshire Blvd, 6th Floor, Suite 620,
Los Angeles, CA 90017
E-mail: joss@telin.co.id

With a courtesy copy, in the case of the Telkom Parties, which shall not constitute adequate communications or notice, to the following, or any other person or persons identified by the Telkom Parties through notice to DOJ after the Effective Date.

Edward A. Yorkgitis, Jr.
Denise N. Smith
Kelley Drye & Warren LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
Fax: (202) 342-8451
E-mail: cyorkgitis@kelleydrye.com; dsmith@kelleydrye.com

ARTICLE VI FREEDOM OF INFORMATION ACT

- 6.1 **Protection from Disclosure:** The DOJ shall take all reasonable measures to protect from public disclosure all information submitted by Telkom USA to the DOJ in connection with this Agreement and clearly marked with the legend:

“Confidential; Subject to Protection Under 5 U.S.C. Section 552(b); Not to be Released Without Notice to PT Telkom, Telin, and Telkom USA,” or similar designation.

Such markings shall signify that it is Telkom USA’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). 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, as appropriate, shall notify Telkom USA of the intended disclosure as provided by Executive Order 12,600, 52 Fed. Reg. 23781 (June 25, 1987). If Telkom USA objects to the intended disclosure and its objections are not sustained, the DOJ, as appropriate, shall notify Telkom USA using the method set forth in Sections 5.15(c) of its intention to release (as provided by Section 5 of Executive Order 12600) not later than **five (5) business days** prior to disclosure of the challenged information.

- 6.2 **Use of Information for USG Purposes:** Nothing in this Agreement or the Implementation Plan shall prevent the DOJ from lawfully disseminating information as appropriate to seek enforcement of this Agreement or the Implementation Plan, provided that the DOJ takes all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

ARTICLE VII OTHER

- 7.1 **Informal Resolution:** The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement or the Implementation Plan. Disagreements shall be addressed by the Parties, in the first instance, at the staff level by their designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to higher authorized officials, unless the DOJ believes that important U.S. interests can be protected, or the Parties believe that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 8.2 below. If, after meeting with higher authorized officials, any Party determines that further negotiations would be fruitless, then any Party may resort to the remedies set forth in Section 8.2 below. If resolution of a disagreement requires Access to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances.
- 7.2 **Enforcement of Agreement and the Implementation Plan:** Subject to Section 8.1 of this Agreement, if any Party believes that any other Party has breached or is about to breach this Agreement or the Implementation Plan, that Party may bring an action against the other Party for appropriate judicial relief. Subject to Article III and Section 7.1, nothing in this Agreement or the Implementation Plan shall limit or affect the right of the DOJ or a USG Authority to:
- (a) seek revocation by the FCC of any license, permit, or other authorization granted or given by the FCC to PT Telkom, Telin, or Telkom USA, or seek any other action by the FCC regarding PT Telkom, Telin, or Telkom USA; or
 - (b) seek civil sanctions for any violation of any U.S. law or regulation or term of this Agreement or the Implementation Plan; or
 - (c) pursue criminal sanctions against PT Telkom, Telin, or Telkom USA or any of its respective directors, officers, employees, representatives or agents, or against any other person or entity, for violations of the criminal laws of the United States.
- 7.3 **Forum Selection:** Any civil action for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement or the Implementation Plan shall be brought, if at all, in the United States District Court for the District of Columbia.
- 7.4 **Choice of Law and Jurisdiction.** This Agreement shall be governed by and interpreted according to the federal laws of the United States. Solely with respect to its obligations under this Agreement, each of the Telkom Parties hereby irrevocably waives, to the fullest extent permitted by law, any immunity from jurisdiction or from any legal process, including attachment or execution, to which it or its property in the United States or its activities or may be entitled on the grounds of sovereignty in any action brought in any

U.S. court in the United States by the United States or by one of its agencies, officers, or instrumentalities.

- 7.5 **Irreparable Injury**: Each of the Telkom Parties agrees that the United States would suffer irreparable injury if for any reason PT Telkom, Telin, or Telkom USA failed to perform any of its significant obligations under this Agreement or, under the Telkom Parties' Implementation Plan, and that monetary relief would not be an adequate remedy. Accordingly, the Telkom Parties each agrees that, in seeking to enforce this Agreement or the Implementation Plan, the DOJ shall be entitled, in addition to any other remedy available at law or equity and pursuant to a valid court order, to specific performance and injunctive or other equitable relief.

ARTICLE VIII

DISPUTES AND MISCELLANEOUS

- 8.1 **Right to Make and Perform Agreement**: The Telkom Parties represent that they have and shall continue to have throughout the term of this Agreement and the Implementation Plan the full right to enter into this Agreement and the Implementation Plan, and to perform their respective obligations hereunder, and that this Agreement and the Implementation Plan are legal, valid, and binding obligations enforceable in accordance with their terms.
- 8.2 **Non-Relinquishment of Rights**: The availability of any civil remedy under this Agreement or the Implementation Plan shall not prejudice the exercise of any other civil remedy under this Agreement, the Implementation Plan, 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 the Implementation Plan, 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, and shall impact the rights of such party to retract, void, or terminate such waiver unless such a right is granted in a waiver.
- 8.3 **Headings**: The article and section headings and numbering in this Agreement and the Implementation Plan are inserted for convenience only and shall not affect the meaning or interpretation of this Agreement or the Implementation Plan.
- 8.4 **Other Laws**: Nothing in this Agreement or the Implementation Plan is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local law or regulation on the Parties; (b) any enforcement authority available under any U.S. federal, state or local law or regulation; (c) the sovereign immunity of the United States; or (d) authority that the DOJ may independently possess over PT Telkom's, Telin's, or Telkom USA's activities or facilities wherever located.

- 8.5 **Statutory References**: All references in this Agreement to statutory provisions shall include any future amendments under Section 8.7 or superseding replacements to such statutory provisions.
- 8.6 **Non-Parties**: Nothing in this Agreement or the Implementation Plan is intended to confer, or does confer, any rights or obligations on any Person other than the Parties and any other Governmental Authority in the United States authorized to effect Electronic Surveillance pursuant to Lawful U.S. Process.
- 8.7 **Modification**: This Agreement and the Implementation Plan may only be modified by written agreement signed by all of the Parties. Any substantial modification to this Agreement shall be reported to the FCC within **thirty (30) days** of the date of the last signature affixed to a written modification of the Agreement by the Parties.
- 8.8 **Release**: Either Party may seek individual releases from specific terms, obligations, or portions of this Agreement by requesting such release from the other Parties. Releases from specific terms, obligations, or portions of this Agreement must be granted in writing to be effective, and can be subject to terms and conditions imposed, or withdrawn at any time, by the granting Party.
- 8.9 **Partial Invalidity**: If any portion of this Agreement or the Implementation Plan is declared invalid by a U.S. court of competent jurisdiction, or by subsequent events affecting the corporate ownership or structure of PT Telkom, Telin, or Telkom USA, this Agreement and the Implementation Plan shall be construed as if such portion had never existed, unless such construction would constitute a substantial deviation from the Parties' intent as reflected in this Agreement.
- 8.10 **Good Faith Negotiations**: The Telkom Parties assert that they in good faith have made an assessment, given the current operations of each of the Telkom Parties and any planned operations, as of the Effective Date, that this Agreement will not be unduly burdensome or adversely affect their competitive position. The DOJ agrees to negotiate in good faith and promptly with respect to any request by PT Telkom, Telin, and/or Telkom USA for modification of this Agreement if the obligations imposed on PT Telkom, Telin, and/or Telkom USA under this Agreement prove to be or become unduly burdensome to PT Telkom, Telin, and/or Telkom USA or adversely affect PT Telkom, Telin, and/or Telkom USA's competitive position, or 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, or public safety concerns. If the DOJ finds that the terms of this Agreement or the Implementation Plan are inadequate to address national security, law enforcement, and public safety concerns presented by an acquisition by Telkom USA in the United States after the date that all the Parties have executed this Agreement, Telkom USA, as applicable, shall negotiate in good faith to modify this Agreement or the Implementation Plan to address those concerns.


- 8.11 **Successors and Assigns:** This Agreement and the Implementation Plan shall inure to the benefit of, and shall be binding upon, PT Telkom, Telin, Telkom USA, the DOJ, and their respective successors and assigns. This Agreement and the Implementation Plan shall apply in full force and effect to any entity or asset, whether acquired before or after the Effective Date, over which the Telkom Parties, including their successors or assigns, has the power or authority to exercise *de facto* or *de jure* control.
- 8.12 **Joint Ventures:** Telkom USA, as of the Effective Date, has not entered into any joint ventures or other arrangements under which a joint venture or another entity may provide DC services. If PT Telkom, Telin, or Telkom USA in the future enter into such joint venture(s) or other arrangement(s) and have the power or authority to exercise *de facto* or *de jure* control over such entity, then PT Telkom, Telin, or Telkom USA, as applicable, will ensure that such entity shall fully comply with the terms of this Agreement and the Implementation Plan. To the extent that PT Telkom, Telin, or Telkom USA lacks such power or authority over such an entity, PT Telkom, Telin, or Telkom USA shall in good faith endeavor to have such entity comply with this Agreement and the Implementation Plan and shall consult with the DOJ about the activities of such entity. For the avoidance of doubt, such joint venture(s) or other arrangements(s) that are the subject of this paragraph shall not include arrangements by which Telkom USA is reselling the services or capacity of another entity.
- 8.13 **Effective Date of Agreement:** Except as otherwise specifically provided in the provisions of this Agreement, the obligations imposed and the rights conferred by this Agreement shall take effect upon the Effective Date.
- 8.14 **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.
- 8.15 **Counterparts:** This Agreement may be executed in one or more counterparts, including by facsimile or portable document format (“PDF”), each of which shall together constitute one and the same agreement.

EXECUTION

This Agreement is executed on behalf of the Parties:

United States Department of Justice

Date: 12/13/2016

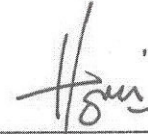
By: 

Printed Name: Richard C. Sofield

Title: Director, Foreign Investment Review Staff

PT Telekomunikasi Indonesia Tbk.

Date: December 13, 2016

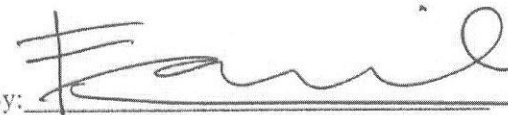
By: 

Printed Name: HONESTI BASYIR

Title: CEO WHOLESALE & INTERNATIONAL BUSINESS

PT Telekomunikasi Indonesia
International

Date: December 13, 2016

By: 

Printed Name: Faizal Rochmad Djoemadi

Title: President Director

Telekomunikasi Indonesia International
(USA) Inc.

Date: December 13, 2016

By: 

Printed Name: Joseph Sahat Raja

Title: Chief Executive Officer