

NATIONAL SECURITY AGREEMENT

This National Security Agreement (“NSA”) is made as of the date of the last signature affixed hereto, by and between GU Holdings Inc. (“GU Holdings”) and Google LLC (“Google”) on the one hand, and the U.S. Department of Justice (“DOJ”), the U.S. Department of Homeland Security (“DHS”), and U.S. Department of Defense (“DOD”), (collectively, “Government Parties” or “Compliance Monitoring Agencies” (“CMAs”)) on the other (each referred to individually as a “Party” and collectively as the “Parties”).

RECITALS

WHEREAS, GU Holdings is an indirect, wholly owned subsidiary of Google;

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

WHEREAS, the United States Government has an obligation to its citizens to ensure that United States communications and related information are secure in order to protect the privacy of United States persons and to enforce the laws of the United States;

WHEREAS, the President of the United States has determined that “foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.” Securing the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019);

WHEREAS, no person shall land or operate in the United States any submarine cable directly or indirectly connecting the United States with any foreign country, unless a written license to land or operate such cable has been issued by the President of the United States, 47 U.S.C. § 34; and the President may withhold or revoke such license after due notice and hearing if doing so will maintain the rights or interests of the United States or of its citizens in foreign countries, or will promote the security of the United States, 47 U.S.C. § 35;

WHEREAS, it is critical to the well-being of the United States and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (*see, e.g.*, Critical Infrastructure Protection in the Information Age, Exec. Order No.13,231, 66 Fed. Reg. 53,063 (October 16, 2001); and Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience);

WHEREAS, GU Holdings and Edge Cable Holdings USA, LLC (“Edge”) seek a license to land and operate within the United States a private fiber-optic submarine cable system



connecting the United States to Taiwan and the Philippines, called the Pacific Light Cable Network (“PLCN”);

WHEREAS, on September 11, 2020, the Federal Communications Commission (“FCC”) referred to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (the “Committee”) an application for a submarine cable landing license, FCC File No. SCL-LIC-20200827-00038 (the “Application”);

WHEREAS, on September 16, 2020, the Committee requested that the FCC defer action on the Application and remove it from streamline for the Committee to review the matter for national security and law enforcement issues; and

WHEREAS, GU Holdings and Google enter into this NSA with the CMAs solely as a condition to the Application, and GU Holdings and Google understand that the CMAs have petitioned the FCC to condition its grant of the Application on compliance with this NSA.

ARTICLE 1. DEFINITIONS

- A. “Access” 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).
- B. “Cybersecurity Incident Response Plan” means a plan or processes put in place to develop and implement the appropriate activities to take action regarding a detected cybersecurity event that has been determined to have an impact on PLCN prompting the need for response and recovery.
- C. “Domestic Communications” means: (a) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States or its territories.
- D. “Domestic Communications Infrastructure” or “DCI” means: (a) any portion of PLCN that is physically located in the United States up to and including the submarine line terminal equipment (“SLTE”), including (if any) transmission, switching, bridging, and routing equipment, and any associated software (with the exception of commercial-off-the-shelf (“COTS”) software used for common

business functions, e.g., Google Workspace or Microsoft Office) used by or on behalf of GU Holdings to provide, process, direct, control, supervise, or manage Domestic Communications, and (b) PLCN Network Operations Center facilities, as defined in Section G below.

- E. “Electronic Communication” has the meaning given to it in 18 U.S.C. § 2510(12).
- F. “Managed Network Service Provider” or “MNSP” means any party or entity other than GU Holdings that provides any of the following functions for the DCI for PLCN: operations and management support; corrective and preventative maintenance, including intrusion testing; network operations and service monitoring; network performance, optimization, and reporting; installation and testing; network audits, provisioning, and development; and the implementation of changes and upgrades.
- G. “Network Management Information” has the meaning defined in Article 2.B.1.a.
- H. “Network Operations Center” or “NOC” means any location or facility used for the purposes of performing network management, monitoring, maintenance, or other operational functions for PLCN.
- I. “PLCN System” means the subsea cable system connecting the United States to Taiwan and the Philippines and all of its associated Principal Equipment.
- J. “Principal Equipment” means the primary electronic components of PLCN that support the subsea cable system end-to-end. This term includes the DCI and Wet Infrastructure/Plant. Principal Equipment also includes, but is in no way limited to:
 - a) network elements such as servers; routers; switches; repeaters; SLTE;
 - b) system supervisory equipment (“SSE”);
 - c) signal modulators and amplifiers;
 - d) power feed equipment (“PFE”);
 - e) tilt and shape equalizer units (“TEQ/SEQ”);
 - f) optical distribution frames (“ODF”);
 - g) branching units (“BU”);
 - h) synchronous optical network (“SONET”);
 - i) synchronous digital hierarchy (“SDH”);
 - j) wavelength selective switch (“WSS”) technology;
 - k) wave division multiplexing (“WDM”);
 - l) dense wave division multiplexing (“DWDM”);
 - m) coarse wave division multiplexing (“CWDM”);
 - n) optical carrier network (“OCx”) equipment, as applicable;

- o) all software used to support PLCN operations and services (with the exception of COTS software used for common business functions, e.g., Google Workspace or Microsoft Office); and
 - p) other equipment, whether physical or logical, that performs the functions of the equipment described in this definition that is being employed or otherwise used on PLCN, or which GU Holdings has definitive plans to employ or otherwise use on PLCN.
- K. “Screened Personnel” has the meaning given it in Article 4, Section C below.
- L. “Security” means a condition that results from the establishment and maintenance of protective measures that enables an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization’s risk management approach.
- M. “U.S. Records” means GU Holdings’ customer billing records, subscriber information, personally identifiable information, sensitive personal data, or any other information used, processed, or maintained in the ordinary course of business related to the services offered by GU Holdings in connection with PLCN, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. §§ 2703(c)-(d) and 18 U.S.C. § 2709.
- N. “U.S.-Taiwan Segment” means Fiber Pair 2 between the United States and Taiwan and any common equipment necessary to its operation.
- O. “Wet Infrastructure” or “Wet Plant” means hardware components installed and residing on the undersea portion of PLCN, including fiber optic cables, repeaters, branching units, and routers (if any). Wet Infrastructure includes all the components used to define the topology of the undersea portion of the U.S.-Taiwan Segment.
- P. “Wire Communication” has the meaning given to it in 18 U.S.C. § 2510(1).

ARTICLE 2. OPERATIONS AND FACILITIES

A. Security Officer; Information Security Officer; Compliance Officer

1. GU Holdings and Google agree to maintain a Security Officer–PLCN System (“Security Officer”) for purposes of this NSA. The Security Officer will be a U.S. citizen residing in the United States, and, to the knowledge of GU Holdings, be

- eligible to hold an active U.S. Government security clearance at the “Secret” level or higher. The Security Officer will possess or have access to the expertise and resources required to assess the physical and logical security of submarine systems, operations of GU Holdings and affiliates that use the PLCN System, PLCN network engineering, and PLCN network security.
2. The Security Officer will establish a communications channel that is available 24 hours per day, 7 days per week to address any national security or law enforcement concerns that the CMAs may raise. Upon request by the CMAs, the Security Officer will make himself/herself available in person within the United States within **72 hours** (except as otherwise agreed under the circumstances), at a date and location, to include in a classified setting, as reasonably deemed necessary by the CMAs. The role of the Security Officer will include receiving and promptly responding to any inquiries or requests for information.
 3. GU Holdings and Google agree to maintain an Information Security Officer–PLCN System (“ISO”) for purposes of ensuring that GU Holdings can address risks identified by the CMAs. The ISO will possess or have access to the appropriate authority, reporting lines, independence, skills, resources, and knowledge about Google’s networks and plans, and who can address Google executives regarding risks identified when necessary.
 4. GU Holdings agrees to maintain a Compliance Officer–PLCN System (“Compliance Officer”) for purposes of ensuring that GU Holdings complies with obligations set forth in this NSA. The Compliance Officer will possess or have access to the appropriate authority, reporting lines, independence, skills, and resources to ensure compliance with the terms of this NSA.
 5. GU Holdings agrees to nominate the proposed Security Officer, ISO, and Compliance Officer within **30 days** of the execution of this NSA. GU Holdings understands that the Security Officer, ISO, and Compliance Officer nominations, which include a proposed change under this Article 2(A)(5), will be subject to the CMAs’ review and approval (or non-objection), which the CMAs will not unreasonably withhold, and may be subject to a background check at the sole discretion of the CMAs. In order to facilitate this, GU Holdings and Google will provide personally identifiable information as needed by the CMAs. Within **30 days** of receipt of the nominations, the CMAs will approve or disapprove the Security Officer, ISO, and Compliance Officer, subject to the tolling provisions in Article 6.2. GU Holdings agrees to notify the CMAs of any proposed change to the Security Officer, ISO, or Compliance Officer at least **10 days** in advance of such proposed change (except in the case of the unavailability, resignation, or death of the Security Officer, ISO, or Compliance Officer in which case such written notice must be provided within **five (5) days** of such event being known to GU Holdings). Absent exigent circumstances or contrary

requirements of law, any planned termination of the employment of the Security Officer, ISO, or Compliance Officer, whether for cause or otherwise, must be submitted with documentation of reason therefor to the CMAs at least **5 days** in advance of such termination.

6. GU Holdings and Google, and the CMAs will mutually continue existing fora for the sharing of information concerning the security of the U.S.-Taiwan Segment and data transiting the U.S.-Taiwan Segment and further develop such fora as appropriate. Within these fora, GU Holdings and Google agree to make available GU Holdings, Google, or affiliate employees with subject matter expertise on relevant security operations and policies and access to escalation to senior management, as reasonably necessary to address CMA concerns regarding any matters set forth in this NSA.

B. Cable System Information

1. Within **60 days** of the execution of this NSA, and, thereafter within **30 days** upon the CMAs' request, GU Holdings agrees to make available the following PLCN System information for the U.S.-Taiwan Segment:
 - a) Network Management Information, including, as follows: (1) a detailed network map that includes physical and logical topology, including any terrestrial facility from the cable landing stations to Points of Presence ("PoPs") or other facilities housing Principal Equipment; (2) network and telecommunications architecture descriptions including all interfaces/interconnections with any other network, and any interconnection points and controlled gateways to the DCI and Wet Infrastructure; (3) network operational plans, processes, and procedures; (4) locations and functions of any NOCs, data centers, PoPs, interexchange facilities, carrier hotel facilities, and main distribution facilities; (5) an organizational chart, to include specific references to the names and positions of officials responsible for operations of the U.S.-Taiwan Segment, and/or senior officials of any third parties performing such duties on behalf of GU Holdings; (6) descriptions of interfaces and connections to PLCN for service offload, disaster recovery, or administrative functions; and (7) a diagram generally depicting the current physical lay-out of the PLCN equipment in the U.S. and Taiwan cable landing stations, PoP, or other facility housing Principal Equipment for the U.S.-Taiwan Segment;
 - b) A complete and current list of all contracts held by GU Holdings or its designees for the operation, maintenance, repair, and security of PLCN; and
 - c) A restoration plan for the Principal Equipment and the Wet Infrastructure for the U.S.-Taiwan Segment.

C. Operational Requirements

1. GU Holdings will have the ability to promptly and effectively interrupt, in whole or in part, traffic to and from the United States on PLCN within twenty-four (24) hours of notice by disabling or disconnecting circuits at the U.S. cable landing station or at other locations within the United States.
2. GU Holdings will configure all necessary systems to ensure it can suspend or interrupt the optical signal or all communications functionality of the PLCN System within the DCI.
3. Pacific Light Data Communications Co., Ltd (“PLDC”) will not have physical or logical Access to branches or any PLCN equipment between or in the United States and Taiwan.
4. Unescorted Access to the DCI will be strictly limited to GU Holdings and/or Edge, and their agents previously identified to the CMAs. Within **60 days** of the execution of this NSA, and, thereafter within **30 days** upon the CMAs’ request, GU Holdings will identify to the CMAs all individuals with current unescorted Access to the DCI. Thereafter, GU Holdings will provide advance notice of any additional individuals proposed for unescorted Access to the DCI. The CMAs will have **30 days** to review and approve the proposed changes. GU Holdings will not authorize unescorted Access for any individuals prior to the foregoing CMA approval. Notwithstanding the foregoing, for unescorted Access to the DCI by any individual necessary to respond to an unforeseen or uncontrollable event and is necessary to ensure the continued operability of the PLCN System (including the U.S.-Taiwan Segment), GU Holdings agrees to provide advance notice to the CMAs of the modification, if practicable. Where providing notice is impracticable, GU Holdings will provide a detailed description of the unescorted Access and the circumstances surrounding the need to provide unescorted Access without prior notice within 10 days of the affording of such unescorted Access to the DCI. Should the CMAs object to the afforded unescorted Access to the DCI, GU Holdings will work in good faith to resolve the objection to the satisfaction of the CMAs. Nothing in this subsection limits the CMAs’ ability to seek enforcement actions or compliance remedies specified elsewhere in this NSA or available by law. GU Holdings will maintain, for a period of at least the previous **18 months**, a log of individuals who have had escorted Access to the DCI.
5. Exclusive authority to permit Access to the SLTE or PFE for PLCN will be vested in GU Holdings and/or Edge and subject to the terms of Article 4.B.3.

6. GU Holdings agrees that this NSA does not authorize connection or operation, for any purposes, of any fiber pairs, or any supporting equipment, originating or terminating in Hong Kong, to include Fiber Pairs 3 through 6 owned by PLDC. GU Holdings will not connect Segments S1.1.1 or S1.1.2 of its Fiber Pair 2, or its Segment S2, directly to any Taiwan-Hong Kong submarine cable or submarine cable segment, including Segments S1.2, S1.3, and S1.4 of the PLCN System. GU Holdings also will not employ any portion of the U.S.-Taiwan Segment in any other configuration that is the equivalent of a direct fiber pair between the United States and Hong Kong.
7. GU Holdings will ensure that PLDC will not operate any equipment or software related to the U.S.-Taiwan Segment. PLDC will not perform network management functions and will not have Access to branches or any other equipment on the U.S.-Taiwan Segment.
8. GU Holdings shall not enter into any agreement under which PLDC and affiliated entities gain a larger percentage interest in PLCN than is held at the time of execution of this NSA.
9. GU Holdings will notify the CMAs of any amendments or changes increasing the rights or responsibilities of PLDC in the September 16, 2016 Joint Build Agreement (“JBA”), as amended, for PLCN **14 days** prior to such amendment or change, and such amendments or changes will be subject to the advance approval of the CMAs, which shall not be unreasonably delayed or denied.
10. Executive Committee under JBA: GU Holdings will provide notice to the CMAs within 5 days of:
 - a) (Material impact) Any notification made to the Executive Committee pursuant to Section 7.14(b) of the JBA; and
 - b) (Upgrade of capacity) Any notification made to the Executive Committee by the Expert Group under Section 14.1(f) of the JBA.Upon request of the CMAs, GU Holdings agrees to meet and confer regarding the item noticed to the CMAs pursuant to this Section, including to discuss any impact to the U.S.-Taiwan Segment or any common equipment necessary to its operation.
11. In addition, GU Holdings agrees to provide advance notice and reasonable opportunity to meet and confer regarding any decision:
 - a) Initiated by PLDC pursuant to Section 7.11 of the JBA; or
 - b) Initiated pursuant to Section 7.11 of the JBA by any other investor on the PLCN System and to which PLDC is the only investor to abstain or decline to support such decision; or
 - c) Called to a vote of the Executive Committee pursuant to Section 7.11 of the JBA;

- provided, however, that the obligation of this Paragraph will not apply when such decision(s) are considered or undertaken in response to an event that is unforeseen or uncontrollable by GU Holdings, such that providing advance notice and opportunity to meet and confer is impracticable. In such cases, GU Holdings will provide within five (5) days a detailed description of the decision(s) considered or undertaken and the circumstances surrounding the need to do so without prior notice and opportunity to meet and confer.
12. GU Holdings will report to the CMAs within 5 days of issuing notice to PLDC of a breach of the JBA that affects the U.S.-Taiwan Segment. Upon CMA request, GU Holdings will meet and confer with the CMAs to discuss information pertaining to the noticed breach.
 13. Shared Operations with PLDC: GU Holdings will ensure PLDC shall not participate in Operations of the U.S.-Taiwan Segment, except as approved by the CMAs. As used in this paragraph, "Operations" means management or supervision of day-to-day activities relating to the performance, maintenance, and repair of the U.S.-Taiwan Segment, including those performed directly or through third-party service providers. Any proposal for participation of PLDC in Operations of the U.S.-Taiwan Segment will be subject to review and approval or disapproval by the CMAs within 45 days of receipt of a proposal submitted by GU Holdings, which shall not be unreasonably withheld.
 14. GU Holdings will ensure that neither PLDC nor its affiliates Access any proprietary information of GU Holdings or Google related to the PLCN System or U.S.-Taiwan Segment. Should GU Holdings seek to supply PLDC data relating to the financial condition of PLCN, it may do so pursuant to approval by the CMAs, which will be provided within **30 days** of the CMAs' receipt of the data. GU Holdings shall respond in writing to written questions that PLDC may have concerning information contained in such reports.
 15. GU Holdings will instruct GU Holdings personnel interfacing with PLDC as to GU Holdings' obligations under the NSA, including individuals' duty to report any violation or any actual or attempted exertion of influence or control by PLDC over GU Holdings, and to issue periodic reminders of such obligations. GU Holdings will issue instructions in writing and provide appropriate live training within **5 days** of the execution of this NSA. GU Holdings will notify the CMAs within **48 hours** if it has reason to believe that PLDC has actually or attempted to exert influence or control over GU Holdings' business or management in a manner intended to adversely affect the performance of PLCN and will confer with the CMAs regarding such influence or control. Upon request of the CMAs, the Security Officer will attend any such conference with the CMAs and provide regular updates to the CMAs regarding actual or attempted exertions of influence noticed to the CMAs pursuant to this Section.

16. GU Holdings and Google will continue to pursue diversification of interconnection points in Asia, including but not limited to Indonesia, Philippines, Thailand, Singapore, and Vietnam. This diversification will include pursuing the establishment of network facilities that allow delivery of traffic on Google's network as close as practicable to the traffic's ultimate destination. Not less than twice in each 12-month period, the ISO will offer the CMAs, at the CMAs' option, a briefing on its measurable steps in pursuit of diversification of interconnection points in Asia consistent with this Section.
17. Within **60 days** of the execution of this NSA, GU Holdings agrees to provide the CMAs notice of the proposed location(s) and, if not GU Holdings, the controller, operator, or manager, for NOC(s) supporting the U.S.-Taiwan Segment. All PLCN NOCs capable of provisioning, managing, configuring, or otherwise Accessing DCI must be physically located in the United States and operated by Screened Personnel as defined below. The CMAs will approve or disapprove the NOC location(s) within **30 days** of receipt or as otherwise agreed to by GU Holdings and the CMAs, with the right of approval not waived unless provided in writing by the CMAs, and subject to the tolling provisions in Article 6.2.
18. GU Holdings will notify the CMAs of any proposed change to NOC location(s), to include the addition of new NOC location(s), and of any proposed change to the controller, operator, or manager for the NOC(s), at least **45 days** in advance of such proposed change. Any proposed or new NOC location will be subject to review and approval or disapproval by the CMAs within **30 days** of receipt or as otherwise agreed to by GU Holdings and the CMAs, with the right of approval not waived unless provided in writing by the CMAs, and subject to the tolling provisions in Article 6.2.

ARTICLE 3. PRINCIPAL EQUIPMENT, VENDORS AND CONTRACTORS

A. Principal Equipment List

1. Definition Supplementation. GU Holdings and the CMAs agree to supplement in writing the foregoing definition of Principal Equipment to address subsequent technological developments with submarine systems.
2. Within **60 days** of the execution of this NSA, GU Holdings agrees to provide the CMAs with a list including the following:
 - a) A complete and current list of all Principal Equipment on the U.S.-Taiwan Segment, including: (1) a description of each item and the functions

supported, (2) each item's manufacturer, and (3) the model and/or version number of any hardware or software;

- b) A complete list of all vendors, contractors, or subcontractors involved in providing, installing, operating, managing, repairing, or maintaining such Principal Equipment, as well as all vendors, contractors, or subcontractors performing service on a NOC supporting the U.S.-Taiwan Segment or U.S. landing station space dedicated to the PLCN System; and
 - c) A repair and maintenance plan for the Principal Equipment used in connection with the U.S.-Taiwan Segment and the Wet Infrastructure/Plant used in connection with the U.S.-Taiwan Segment.
3. The CMAs will approve or disapprove the Principal Equipment List within **60 days** of receipt, subject to the tolling provisions in Article 6.2.

In the event of a disapproval, GU Holdings will not initiate or expand the existing deployment of or reliance on, and will not enhance the capabilities of, any Principal Equipment of which the CMAs have disapproved. GU Holdings will meet, confer, and otherwise attempt in good faith to resolve the CMAs' reason for disapproval. Until the CMAs' rationale for disapproval is resolved, GU Holdings will not upgrade, install, replace, or service any disapproved Principal Equipment without written authorization from the CMAs.

B. Modifications to Existing Principal Equipment and Vendors, Contractors, and Subcontractors

1. Except as provided in subsection 3 of this Section, GU Holdings will provide the CMAs at least **15 days'** advance notice prior to performing any maintenance, repair, or replacement that would result in any modification to the quantum, function, configuration, operation, or location of a.) existing Principal Equipment used in connection with the U.S-Taiwan Segment, b.) a NOC supporting the U.S.-Taiwan Segment, c.) U.S. landing station space dedicated to the PLCN System, or d.) branching unit or cable equipment, as items a.) through d.) have been described to the CMAs.
2. GU Holdings will provide at least **30 days'** notice prior to any change to the list of vendors, contractors, or subcontractors involved in providing, installing, operating, managing, repairing, or maintaining the Principal Equipment and those performing service on a NOC supporting the U.S.-Taiwan Segment or U.S. landing station space dedicated to the PLCN System. This will include any change to the service offerings or support from a previously listed vendor, contractor, or subcontractor (*i.e.*, where a previously listed provider will be offering support in a previously unidentified way).

3. For any maintenance, repair, or replacement that is undertaken in response to an unforeseen or uncontrollable event and is necessary to ensure the continued operability of the Principal Equipment used in connection with the U.S.-Taiwan Segment, GU Holdings agrees to provide advance notice to the CMAs of the modification, if practicable. Where providing notice is impracticable, GU Holdings will provide a detailed description of the maintenance, repair, or equipment replacement and the circumstances surrounding the need to conduct such activity without prior notice within **10 days** of the maintenance, repair, or replacement. Should the CMAs object to the undertaken activity, GU Holdings will work in good faith to resolve the objection to the satisfaction of the CMAs. Nothing in this subsection limits the CMAs' ability to seek enforcement actions or compliance remedies specified elsewhere in this NSA or available by law.
4. The CMAs will approve or disapprove any notice submitted pursuant to this Section within **30 days** of receipt, subject to the tolling provisions in Article 6.2.

In the event of a disapproval of the performance of maintenance, repair, or replacement of Principal Equipment under Article 3.B.1, GU Holdings will not initiate or expand the existing deployment of or reliance on, and will not enhance the capabilities of, any Principal Equipment of which the CMAs have disapproved. In the event of a disapproval of any change to the list of vendors, contractors, or subcontractors under Article 3.B.2, GU Holdings will not permit such disapproved vendor, contractor, or subcontractor to provide, install, operate, manage, repair, or maintain any Principal Equipment. GU Holdings will meet, confer, and otherwise attempt in good faith to resolve the CMAs' reason for disapproval. Until the CMAs' rationale for disapproval is resolved, GU Holdings will not initiate the notified change without written authorization from the CMAs.

C. Principal Equipment Testing

1. GU Holdings will notify the CMAs at least **30 days** prior to initiating the testing of any new Principal Equipment used in connection with the U.S.-Taiwan System by any vendor not already on the approved Principal Equipment List.
2. The CMAs will approve or disapprove the proposed testing within **30 days** of receipt.

In the event of a disapproval, GU Holdings will not initiate the notified testing and will meet, confer, and otherwise attempt in good faith to resolve the CMAs' reason for disapproval.

3. Prior to deployment of any distributed acoustic sensing technology onto the marine portion of this cable, GU Holdings agrees to receive the approval of the United States Navy. GU Holdings will provide notice to the United States Navy via email at osd.pentagon.ousd-a-s.list.team-telecom@mail.mil prior to the deployment, with a

courtesy copy to DHS, DOD, and DOJ. The United States Navy will approve or disapprove the deployment within **45 days** of receipt.

D. Managed Network Service Providers

1. GU Holdings will identify MNSPs, whether in the United States or elsewhere, who will provide services to the U.S.-Taiwan Segment at least **60 days** before any services are performed. Such notification will describe the service offerings or support offered by the MNSP.
2. GU Holdings will notify the CMAs at least **60 days** prior to any change to the service offerings or support from a previously notified MNSP.
3. The CMAs will approve or disapprove any MNSP or any modification to the service offerings within **60 days** of receipt, subject to the tolling provisions in Article 6.2.

ARTICLE 4. USE, ACCESS AND SECURITY

A. Preventing Improper Use and Unauthorized Logical Access

1. GU Holdings will take practicable measures to prevent unauthorized logical Access to the PLCN System; Wet Infrastructure; and DCI used in the U.S.-Taiwan Segment, and to prevent any unlawful use or disclosure of information while carried on the same, including Domestic Communications, and GU Holdings will include these measures in the policies that it develops and implements pursuant to this NSA. For purposes of this Section, “practicable measures,” at a minimum, includes measures equal, comparable, or superior to generally recognized industry standards governing cybersecurity, information security, and privacy and will be measured consistent with best practices and guidelines, such as but not limited to the Cybersecurity Framework of the National Institute of Standards and Technology and 27001 Series Standards of the International Organization for Standardization. These practicable measures should also include items such as configuration management, security audits, and system interconnection documentation, as well as contractual safeguards and screening procedures for personnel with logical Access to the DCI.
2. GU Holdings will take appropriate measures to protect and promote resiliency of PLCN, including measures to ensure that security patches for systems and applications are up to date.
3. GU Holdings will maintain or exceed security standards and best practices utilized within the U.S. telecommunications industry for maintenance of password systems and firewalls, monitoring and oversight of logical Access to PLCN, adequate

maintenance of logical Access logs, and periodic internal audits of network security and associated network devices. GU Holdings agrees that its security standards and practices for PLCN will also include, among other things, policies or plans relating to its information security, supply chain security, cybersecurity incident response, remote Access, cybersecurity, third-party contractors, outsourcing and offshoring, maintenance and retention of system logs, protection of lawful U.S. process, protection of U.S. Records obtained by GU Holdings in the ordinary course of business, and GU Holdings' plans regarding new contracts or amendments to existing contracts with third-party providers requiring those third parties to notify GU Holdings in the event of a breach or loss of U.S. Records within a specified time period after discovery, not to exceed **72 hours** from the time of discovery, unless the CMAs grant a waiver.

4. Within **60 days** of the execution of this NSA, GU Holdings will submit to the CMAs a policy setting forth its logical security measures adopted in accordance with the requirements of this Article 4, Section A. Within 90 days of receipt, the CMAs will approve or disapprove the policy. GU Holdings agrees that the policy will be updated, when appropriate, to conform with evolving information security standards and that GU Holdings will, if requested by the CMAs, address in the policy any additional concerns raised by the CMAs to GU Holdings in writing and work with the CMAs to implement any related modifications. GU Holdings will, within 5 days, submit any material changes to the policy for review and approval or disapproval by the CMAs, which shall occur within **90 days** of receipt, subject to the tolling provision in Article 6.2.

B. Physical Security Measures

1. GU Holdings will take practicable measures to physically secure the U.S.-Taiwan Segment, including the DCI and Wet Infrastructure. GU Holdings will screen appropriate persons in accordance with Article 4, Section C, and GU Holdings will require that all persons who physically Access the DCI are escorted at all times by Screened Personnel. GU Holdings will maintain physical Access logs and will provide such logs upon the CMAs' request.
2. Within **60 days** of the execution of this NSA, GU Holdings will submit to the CMAs a policy setting forth its physical security measures. Within **90 days** of receipt, the CMAs will approve or disapprove the Physical Security Policy, subject to the tolling provisions in Article 6.2. GU Holdings will, within 5 days, submit any material changes to the Physical Security Policy for review and approval or disapproval by the CMAs, which shall occur within **90 days** of receipt.

3. Within **30 days** of the execution of this NSA, and thereafter within **five (5) days** of a request by the CMAs, GU Holdings will provide the CMAs with a list of all persons, vendors, contractors, subcontractors, or other entities who have been granted unescorted Access to the U.S.-Taiwan Segment and any PLCN System DCI, including identifying the applicable facilities to which such persons, vendors, contractors, or entities have been granted unescorted Access and the type of services or support offered by such persons, vendors, contractors, or entities. The CMAs may object to any persons, vendors, contractors, or entities on the list and will do so within **90 days** of receipt. In the event of any such objection, GU Holdings agrees to prohibit any such persons, vendors, contractors, or entities from any further physical Access to the DCI or U.S.-Taiwan Segment. Any additions to the list will be subject to CMA approval.
4. Limitation on Access by PLDC: GU Holdings (or any of its controlled entities) will not locate its individual equipment or common equipment for the U.S.-Taiwan Segment in any space owned by PLDC or a PLDC affiliate, or to which PLDC has physical Access, unless approved in advance by the CMAs. Upon CMA request, GU Holdings shall provide maps and floor plans showing where GU Holdings occupies space for the U.S.-Taiwan Segment in each facility.

C. Screening Process

1. Within **60 days** of the execution of this NSA, GU Holdings will submit to the CMAs a screening policy that will include, at a minimum, criminal background checks, public records check, and other generally accepted industry standards to ascertain a person's trustworthiness for the following circumstances:
 - a) Any person whose position could involve logical Access to the DCI; and
 - b) Any person charged with securing the DCI (collectively "Screened Personnel").
2. The CMAs will approve or disapprove the screening policy within **90 days** of receipt, subject to the tolling provisions in Article 6.2. If GU Holdings utilizes a vendor or service provider, the selection of the vendor or service provider is also subject to review and approval by the CMAs. GU Holdings agrees to cooperate with any request by the CMAs to provide additional identifying information regarding Screened Personnel.
3. GU Holdings will itself (or arrange for a third party to) provide the CMAs a list of all Screened Personnel within **30 days** of the CMAs' approval of the screening policy and thereafter upon the CMAs' request. Such list will include:

- a) full name (last, first, middle name);
 - b) other names and aliases used;
 - c) current address;
 - d) country and city of residence;
 - e) date of birth and place of birth;
 - f) social security number (where applicable);
 - g) national identity number, including nationality, date and place of issuance, and expiration date (where applicable);
 - h) passport number (if more than one, all must be fully disclosed), nationality, date and place of issuance, and expiration date and, if a U.S. visa holder, the visa type and number, date and place of issuance, and expiration date; and
 - i) dates and nature of foreign government service (where applicable).
4. The CMAs will approve or disapprove the list within **60 days** of receipt, subject to the tolling provisions in Article 6.2. In the event of an objection to any person on the list, GU Holdings agrees to promptly remove any such person from the list of Screened Personnel and immediately terminate all physical and logical Access.

ARTICLE 5. REPORTING OBLIGATIONS

A. Reporting Incidents and Breaches

1. GU Holdings agrees to report in writing to the CMAs within **48 hours** if it learns of information that reasonably indicates any of the following incidents and/or attempted incidents in connection with the U.S.-Taiwan Segment:
 - a) Unauthorized Access to, or disruption or corruption of, PLCN or any information being carried on PLCN;
 - b) Disruption, shunt faults, or unplanned cable outages as reported to the FCC;
 - c) Any unauthorized physical Access to the U.S. cable landing station or any NOC(s);
 - d) Any unauthorized Access to or disclosure of Network Management Information;
 - e) Any other unauthorized Access to or disclosure of Domestic Communications on PLCN in violation of federal, state, or local law;
 - f) Any material breach of the commitments made in this NSA; or
 - g) Any one or more of the following which affect GU Holdings' or Google's computer network(s) or associated information systems in connection with PLCN:
 - i. Unauthorized disruptions to a service or denial of a service;
 - ii. Unauthorized processing or storage of data;

- iii. Unauthorized modifications to system hardware, firmware, or software, including the identification of vulnerabilities introduced through a cyber supply chain compromise;
 - iv. Unplanned incidents that cause activation of GU Holdings' Cybersecurity Incident Response Plan;
 - v. Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect GU Holdings' ability to comply with the terms of this NSA; or
 - vi. An unauthorized occurrence that (a) actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system; or (b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
2. GU Holdings agrees to require any of its third-party service providers for PLCN to disclose to GU Holdings any security breach in connection with PLCN, whether from data breach or other cause, within **48 hours** of the third party discovering the breach, unless the CMAs grant a waiver. GU Holdings further agrees to require any of its third-party service providers for PLCN to disclose to GU Holdings, within **48 hours** of discovery, unless the CMAs grant a waiver, any critical exposure, threat, and vulnerabilities activating its Cybersecurity Incident Response Plan, associated with the products or services provided to GU Holdings for PLCN that are the result of tainted software, the introduction of malware, the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software and hardware into such products or services or into the third-party providers' supply chain.
3. GU Holdings agrees that, absent an express written grant by the CMAs of an applicable exception, it will require the NOC and cable landing station service providers, by contract, to report within **48 hours** any incident that GU Holdings must report to the CMAs under Article 5.A.1.
4. GU Holdings will submit in writing a follow-up report describing in greater detail the incident or breach and GU Holdings' steps to remediate that incident or breach to the CMAs within **15 days** of discovery of the relevant conduct. GU Holdings will also submit in writing supplementary information regarding any follow-up report until such evaluation is complete. GU Holdings will remediate any incidents or breaches reported pursuant to this Section to the satisfaction of the CMAs.

B. Instruction of Obligations and Reporting Policy

1. GU Holdings will instruct appropriate officers, employees, contractors, and agents as to their obligations under this NSA, including individuals' duty to report any violation, and to issue periodic reminders of such obligations. GU Holdings will issue instructions in writing and provide appropriate live training within **90 days** of the execution of this NSA, and GU Holdings will submit a copy to the CMAs at the same time. GU Holdings agrees to issue updated instructions or training annually thereafter.
2. GU Holdings will adopt and distribute to the management of GU Holdings and relevant management of Google, a written policy for the reporting by the management of GU Holdings and Google of any noncompliance with this NSA. This written policy shall also provide for the reporting by any employees, agents, and contractors to the management of GU Holdings of information that requires notice under this NSA. GU Holdings will make such policy available to the CMAs upon request.
3. GU Holdings shall notify all relevant employees, contractors, and agents of the obligations arising under this Agreement. The written statement informing employees, contractors, and agents of the need to report this information shall also state that GU Holdings will not discriminate against, or otherwise take adverse action against, anyone who reports such information to the management of GU Holdings or the United States Government.

C. Change in Control and Foreign Influence

1. If GU Holdings learns of any information that indicates to GU Holdings that any foreign entity or individual, other than those already identified, has or likely will obtain an ownership interest, whether direct or indirect, in GU Holdings or the PLCN System above five (5) percent, or if any foreign entity or individual, singly or in combination with other foreign entities or individuals, has or likely otherwise will gain either: (i) control, as determined in accordance with 47 C.F.R. § 63.09(b); or (ii) *de facto* or *de jure* control of GU Holdings or PLCN, GU Holdings agrees to provide notice in writing to the CMAs within **10 days**. Notice under this Section will, at a minimum:
 - a) Identify the entity(ies) or individual(s) acquiring control;
 - b) Identify the beneficial owners of any such increased or prospective increased ownership interest in GU Holdings or the PLCN System by the entity(ies) or individual(s); and
 - c) Quantify the amount of ownership interest that the entity(ies) or individual(s) has or likely will obtain in GU Holdings or the PLCN System and, if applicable, the basis for their prospective control of GU Holdings or the PLCN System.

2. GU Holdings will provide notice in writing to the CMAs within **10 days** if GU Holdings learns of any information that indicates that any foreign government, any foreign government-controlled entity, or any foreign entity plans to participate or has participated in any aspect of the day-to-day management of GU Holdings or PLCN in such a way that:
 - a) materially interferes with or impedes the performance by GU Holdings of its duties and obligations under the terms of this NSA;
 - b) materially interferes with or impedes the exercise by GU Holdings of its rights under the NSA;
 - c) raises a material concern with respect to the successful fulfillment by GU Holdings of its obligations under this NSA; or
 - d) materially interferes with or impedes the operation of the PLCN System.

Such notice shall include a description of the timing and the nature of the foreign government's or entity's plans or actions.

D. Annual Report

1. On the anniversary of the date of this NSA, GU Holdings will submit to the CMAs an annual report assessing its compliance with the terms of this NSA for the preceding year.
2. The CMAs may specify certain content, relating to compliance with the terms of this NSA, to be included in a given year's annual report, but at a minimum, the report will include:
 - a) The names and contact information of the then-current Security Officer, ISO, and Compliance Officer;
 - b) Cable System Information, as described in Article 2.B, above, noting any changes during the reporting period;
 - c) An updated Principal Equipment List containing all information described in Article 3.A, identifying any modifications during the reporting period;
 - d) A copy of the then-current policies adopted in accordance with this NSA, including policies for logical security, physical security, personnel screening, incident reporting, and employee training, and a summary of any changes during the reporting period and the reasons therefor;
 - e) A list of all Screened Personnel;

- f) Updated list of all persons, vendors, contractors, or other entities that have been granted unescorted physical Access to any DCI or Principal Equipment in connection with the U.S.-Taiwan Segment;
- g) GU Holdings will certify that shared operations and communications with PLDC do not circumvent the requirements of this NSA as outlined in Articles 2 and 4;
- h) A summary of any events that occurred during the reporting period that will or reasonably could impact the effectiveness of or compliance with this NSA; and
- i) A summary of any known acts of noncompliance with the terms of this NSA that occurred during the reporting period, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future.

E. Risk Assessment

1. GU Holdings and Google will provide the CMAs annual risk assessments addressing the operation and use of the U.S.-Taiwan Segment. Specifically, GU Holdings and Google will conduct annual assessments of the risk to sensitive data that transits the cable, including when the data exits the cable, and will provide the assessments to the CMAs. Sensitive data includes data of U.S. persons, companies, and other entities, and the Parties will use reasonable efforts to identify relevant risks in the assessments. The first annual assessment will be provided to the CMAs no later than 12 months after the execution of this NSA.

F. Third-Party Audit

1. At their sole discretion, but no more than once every calendar year unless the original audit is found by the CMAs to have been unsatisfactory, the CMAs may request a third-party audit of GU Holdings' compliance with the terms of this NSA.
2. The auditor will be subject to the CMAs' approval. Within **60 days** of the CMAs requesting a third-party audit, GU Holdings will nominate two (2) third-party auditor firms to the CMAs. Within **60 days** of the nominations, the CMAs will approve or disapprove the nominated third-party auditor firms.
 - a) GU Holdings may select any auditor approved by the CMAs.

- b) If the CMAs disapprove of either of the nominated third-party auditors, GU Holdings will nominate, within **30 days** of the final decision by the CMAs, another third-party auditor. If the CMAs disapprove the nomination of a supplemental third-party auditor, GU Holdings will provide to the CMAs three (3) additional candidates within **30 days** to be considered for third-party auditor from which the CMAs may choose at their discretion.
 - c) As part of the auditor nomination and approval process, the CMAs may condition approval of a nominated auditor on GU Holdings providing information regarding its and the nominated auditor's pre-existing relationship (if any).
3. GU Holdings will be responsible for any costs associated with any third-party audit carried out pursuant to this Section. The CMAs will consider avoidance of unreasonable costs as a factor when exercising their rights under this Section.
4. GU Holdings will ensure the selected third-party auditor submits, prior to commencing the audit, a methodology and proposed scope of audit, both of which will be subject to the CMAs' approval. The selected third-party auditor will not commence the audit until the CMAs approve the methodology and scope of the audit.
5. GU Holdings will ensure that the executed engagement agreement and all compensation terms with the third-party auditor are provided to the CMAs within **five (5) days** of execution.
6. The third-party auditor will promptly deliver all reports and related information generated or gathered during its review that relate directly to GU Holdings' compliance with the terms of this NSA to GU Holdings and the CMAs and will meet independently with the CMAs upon request.
7. GU Holdings will ensure that the audit includes an evaluation of the Risk Assessment outlined in Article 5.E. that GU Holdings provides to the CMAs.

G. Consultation and Site Visits

1. GU Holdings will work in good faith to resolve to the satisfaction of the CMAs any concerns the CMAs may raise about materials submitted pursuant to this NSA.
2. GU Holdings will work in good faith to resolve to the satisfaction of the CMAs any national security or law enforcement concerns the CMAs may identify with respect to any matters set forth in this NSA.
3. GU Holdings agrees that, upon **48 hours** advance notice, except when due to exigent circumstances such advance notice is not practicable, the CMAs may visit any part of the PLCN facilities to conduct on-site reviews to verify the implementation of and

compliance with the terms of this NSA. During such visits, GU Holdings will provide unimpeded access to any information, facilities, and personnel necessary to verify compliance with the terms of this NSA, on the understanding that when advance notice of a visit is not provided, GU Holdings will provide the CMAs access to information, facilities, and personnel within **24 hours** of receipt of such a request.

4. GU Holdings and Google agree to permit disclosure of confidential and highly confidential information submitted to the FCC pursuant to 47 C.F.R. § 0.442 to federal government departments, agencies, and offices whose principals are listed in Section 3 of Executive Order 13913.

H. FCC Certifications:

1. GU Holdings will, for the U.S.-Taiwan Segment, following the effective date of such requirement under 47 C.F.R. § 63.18 (including any amendments made pursuant to FCC 20-133, released Oct. 1, 2020):
 - a) Comply with all applicable Communications Assistance for Law Enforcement Act (“CALEA”) requirements and related rules and regulations, including any and all FCC orders and opinions governing the application of CALEA, pursuant to the Communications Assistance for Law Enforcement Act and the FCC’s rules and regulations in part 1, subpart Z—Communications Assistance for Law Enforcement Act;
 - b) Make communications to, from, or within the United States, as well as records thereof, available in a form and location that permits them to be subject to a valid and lawful request or legal process in accordance with U.S. law, including but not limited to: (1) the Wiretap Act, 18 U.S.C. § 2510 et seq.; (2) the Stored Communications Act, 18 U.S.C. § 2701 et seq.; (3) the Pen Register and Trap and Trace Statute, 18 U.S.C. § 3121 et seq.; and (4) other court orders, subpoenas, or other legal process;
 - c) Designate a point of contact who is located in the United States and is a U.S. citizen or lawful U.S. permanent resident for the execution of lawful requests and as an agent for legal service of process; and
 - d) Notify the FCC and the CMAs of any changes in the authorization holder or licensee information and/or contact information promptly, and in any event within 30 days.
2. GU Holdings understands that if GU Holdings fails to fulfill any of the conditions and obligations set forth in the certifications set out in subsection 1 of this Section H and/or that if the information provided to the United States Government is

materially false, fictitious, or fraudulent, GU Holdings may be subject to all remedies available to the United States Government, including but not limited to revocation and/or termination of the FCC's authorization or license, and criminal and civil penalties, including penalties under 18 U.S.C. 1001.

3. In the event that the President, the FCC, or the Office of Management and Budget rejects or abandons some or all of the amendments to 47 C.F.R. § 63.18 made pursuant to FCC 20-133, released Oct. 1, 2020, the CMAs and GU Holdings will meet and confer on whether circumstances warrant amendment of subsection 1 of this Section H.

ARTICLE 6. GENERAL PROVISIONS

1. **Computation of Time:** For purposes of counting days in this NSA, the day of the event that triggers the period is excluded, but every day thereafter is counted, including intermediate Saturdays, Sundays, and legal holidays. Include the last day of the period, but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or legal holiday.
2. **Tolling of Deadlines.**
 - a) Any approval provision applicable to the CMAs pursuant to this NSA shall be tolled during a lapse in appropriations or any other time when the federal government in the greater Washington, D.C., area is closed.
 - b) Should the CMAs seek additional information within any period in which they review a submission by GU Holdings for approval or non-objection, the CMAs' objection period will be extended by the number of days the CMAs awaited the complete requested information, and only in that event will the CMAs be deemed to have approved if they do not object within the extended period.
3. **Future Corporate Forms:** This NSA shall be binding upon GU Holdings and Google and their successors, assigns, subsidiaries, and affiliates that have control, access, influence, or authority over the licensed cable system. GU Holdings will not assign any obligation under this NSA without the prior written consent of the CMAs, and GU Holdings will remain responsible for the activities of any person to whom it assigns any obligations under this NSA.
4. **Breach.**

- a) GU Holdings agrees that, in the event GU Holdings breaches the commitments set forth in this NSA, to include conduct contrary to any timely objection from the CMAs to any notice submitted pursuant to this NSA, the Committee may request that the FCC take action consistent with subsection 9(b) of the Executive Order, such as to modify, condition, revoke, cancel, terminate, or render null and void any relevant license, permit, or other authorization granted by the FCC to GU Holdings or any successors-in-interest, in addition to any other remedy available at law or equity.
 - b) GU Holdings and Google agree that the CMAs may request that the FCC take other action including declaratory relief, or request that the FCC impose any other appropriate sanction, including but not limited to, disabling of the U.S.-Taiwan Segment, a forfeiture, or other monetary penalty.
 - c) GU Holdings and Google agree that the CMAs may seek civil sanctions for any violation by GU Holdings of any U.S. law or regulation or term of this NSA, including, but in no way limited to, disabling of the U.S.-Taiwan Segment, specific performance, or injunctive relief.
 - d) GU Holdings and Google agree that the CMAs may pursue criminal sanctions against GU Holdings or any PLCN Party, or any officer, director, employee, contractor, or agent of GU Holdings, or against any other person or entity, for violations of the criminal laws of the United States.
 - e) GU Holdings and Google agree that the CMAs may seek suspension or debarment of GU Holdings from eligibility for contracting with the U.S. Government in accordance with applicable law and regulation.
5. Notices: Following the effective date, all notices and other communications given or made relating to this NSA shall be in writing and shall be deemed given as of the date of receipt and shall be sent by electronic mail to the Parties' designated representatives at the addresses shown below, or in a subsequent notice. If requested by the CMAs, GU Holdings will provide a copy by one of the following methods: (a) personal delivery; (b) documented overnight courier service; or (c) registered or certified mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such addresses as the Parties may designate in accordance with this Section.

If to the CMAs:

U.S. Department of Justice
Attention: Eric S. Johnson and Loyaan A. Egal

National Security Division
Foreign Investment Review Section
175 N Street, NE
Washington, DC 20530
Compliance.Telecom@usdoj.gov

U.S. Department of Homeland Security
Attention: Brien Beattie and Alton Turner
Office of Strategy, Policy, and Plans
Mail Stop 0445
2707 Martin Luther King Avenue, SE
Washington, DC 20528
ip-fcc@hq.dhs.gov

U.S. Department of Defense
Attention: Andrew Pahutski
Director, Foreign Investment Review
Office of the Undersecretary of Defense, Acquisition & Sustainment
3330 Defense Pentagon
Rm 3C759
Washington, DC 20301
osd.pentagon.ousd-a-s.list.team-telecom@mail.mil

If to GU Holdings:

GU Holdings Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
guhholdings-notices@google.com

6. Changed Circumstance: If, after this NSA takes effect, the CMAs or Google and GU Holdings believe that changed circumstances warrant modifying or terminating this NSA (including, but in no way limited to, if the CMAs determine that the terms of this NSA are inadequate or no longer necessary to address national security or law enforcement concerns), GU Holdings and Google and the CMAs agree to negotiate in good faith to address the concerns arising from any changed circumstances. Rejection of a proposed modification alone shall not constitute evidence of a failure to negotiate in good faith. If the CMAs determine that the terms of this NSA are inadequate or no longer necessary to address national security or law enforcement concerns, GU Holdings will address those concerns to the satisfaction of the CMAs. Without limitation, if PLDC ceases to have an ownership interest in the PLCN System, the CMAs will meet, confer, and otherwise attempt in good faith to agree on amendments to this NSA.

7. Continuing Obligations: Nothing in this NSA is intended to excuse GU Holdings or Google from their obligations to comply with all applicable legal requirements and obligations, including all applicable statutes, regulations, requirements, or orders.
8. Irreparable Injury: GU Holdings agrees that the United States would suffer irreparable injury if for any reason GU Holdings failed to perform any of its obligations under this NSA, and that monetary relief would not be an adequate remedy. Accordingly, GU Holdings agrees that, in seeking to enforce this NSA, the Government Parties shall be entitled, in addition to any other remedy available at law or equity, to seek specific performance and injunctive or other equitable relief.
9. Waiver of Immunity: GU Holdings and Google agree that, to the extent that they or any of their property (including FCC licenses and authorizations and intangible property) is or becomes entitled at any time to any immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of a "Foreign State" (as defined in 18 U.S.C. § 1603) from any legal action, suit, or proceeding or from setoff or counterclaim relating to this NSA, from the jurisdiction of any competent court or the FCC, from service of process, from attachment prior to judgment, from attachment in aid of execution of a judgment, from execution pursuant to a judgment or arbitral award, or from any other legal process in any jurisdiction, they, for themselves and their property expressly, irrevocably, and unconditionally waive, and agree not to plead or claim, any such immunity with respect to matters arising with respect to this NSA or the obligations herein (including any obligation for the payment of money) in any proceeding brought by a federal, state, or local U.S. Government Authority. GU Holdings and Google agree that the waiver in this provision is irrevocable and is not subject to withdrawal in any jurisdiction or under any statute, including the Foreign Sovereign Immunities Act, 28 U.S.C. § 1602 *et seq.* The foregoing waiver shall constitute a present waiver of immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of a foreign state at any time any action is initiated by a federal, state, or local U.S. Government Authority against GU Holdings with respect to compliance with this NSA.
10. Forum Selection: It is agreed by and between the Parties that a civil action among the Parties for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this NSA shall be brought, if at all, in the United States District Court for the District of Columbia. GU Holdings and Google expressly waive any personal jurisdiction defenses under 47 U.S.C. § 36 to an action in the United States District Court for the District of Columbia brought by the United States or its agencies.

11. Other Laws: Nothing in this NSA is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local laws on any Party; (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority the U.S. Government may possess over the activities or facilities of GU Holdings located within or outside the United States (including authority pursuant to the International Emergency Economic Powers Act). Nothing in this NSA is intended to or is to be interpreted to require the Parties to violate any applicable law.
12. Entire Agreement: This NSA constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, of the Parties with respect to such subject matter. This NSA may only be modified by written agreement signed by all of the Parties. Any such modification to this NSA shall be reported to the FCC within **30 days** after approval in writing by the Parties.
13. Severability: The provisions of this NSA shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this NSA or the application of any provision thereof.
14. Effectiveness of Agreement: Except as otherwise specifically provided in the provisions of this NSA, the obligations imposed and rights conferred by this NSA shall take effect upon the date this NSA is signed by the last Party to sign it.
15. No Prejudice to Subsequent Proceedings or Agreements: This NSA in whole or in part shall not constitute a waiver of or prejudice to any position taken or adopted by any Party in any subsequent proceeding or negotiation.
16. Notification to FCC: Upon execution of this NSA, the Government Parties will timely notify the FCC that the previously stated condition on the Government Parties' non-objection to the FCC's grant of the license to operate the PLCN System has been satisfied.
17. Counterparts: This NSA may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same NSA.
18. Application to Google: For avoidance of doubt, the provisions of this NSA shall apply to Google LLC only to the extent expressly stated in this NSA.

[Remainder of this page intentionally left blank]

For GU Holdings Inc.:

By: 

Name: Brian Quigley

Title: Authorized Signatory

Date: December 10, 2021



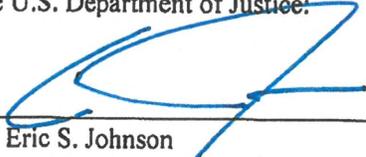
For Google LLC:

DocuSigned by:
By:  _____
Name: Ken Yi C8564282FBC44EB...
Title: Authorized Signatory
Date: 12/10/2021



Agreed to on the last date written below.

For the U.S. Department of Justice:

By: 

Name: Eric S. Johnson

Title: Deputy Chief, National Security Division, Foreign Investment Review Section

Date: 13 Dec 2021

For the U.S. Department of Homeland Security:

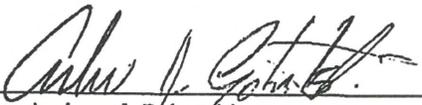
By: 

Name: Kelli Ann Burriesci

Title: Deputy Under Secretary, Office of Strategy, Policy, and Plans

Date: 12.14.21

For the U.S. Department of Defense:

By: 

Name: Andrew J. Pahutski

Title: Director, Foreign Investment Review

Date: 13 DEC 2021