Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
GU Holdings, Inc.; RTI Solutions Inc.; RTI JGA Pte. Ltd.; RTI Connectivity Pte. Ltd.; and AARNet Pty. Ltd.	)	File No. SCL-LIC-20190502-00016
	)	
Application for a License to Land and Operate Within the United States a Submarine Cable Network Connecting Guam and Japan	)	

PETITION TO ADOPT CONDITIONS TO AUTHORIZATION AND LICENSE

Pursuant to Executive Order 13913, the National Telecommunications and Information Administration (NTIA) submits this Petition to Adopt Conditions to Authorization and License (Petition) on behalf of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee).[1] Through this Petition, and pursuant to Section 1.41 of the Commission's Rules, the Committee advises the Commission that it has no objection to the Commission approving the above-captioned application, provided that the Commission conditions its approval on the assurances of GU Holdings, Inc., RTI Solutions Inc., RTI JGA Pte. Ltd., RTI Connectivity Pte. Ltd., and AARNet Pty. Ltd., (collectively, the parties), to abide by the commitments and undertakings set forth in the July 3, 2020 National Security Agreement (NSA), a copy of which is attached hereto.[2]

[1] Exec. Order No. 13913, § 9(h), 85 Fed. Reg. 19643, 19647-48 (2020). The Executive Order directs the Committee to "assist the [Commission] in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector." *Id*. § 3(a), 85 Fed. Reg. at 19643.
[2] 47 C.F.R. § 1.41.

Section 2 of the Cable Landing License Act authorizes the President to withhold, revoke, or condition a submarine cable landing license if the President determines that such action would, among other things, "promote the security of the United States."[3] In 1954, the President delegated that authority to the Commission, subject to a requirement that it not act on an application without first obtaining "such advice from any executive department or establishment of the Government as the Commission deems necessary."[4] The Commission has long sought the expertise of the relevant Executive Branch agencies and has routinely granted agencies' requests to impose conditions on cable landing licenses to address national security, law enforcement and other concerns raised by particular applications.[5]

After discussions with representatives of the parties in connection with the above-captioned application, the Committee has concluded that the additional commitments and undertakings set forth in the NSA will help ensure that those agencies with responsibility for protecting national security, enforcing the law, and preserving public safety can proceed appropriately to satisfy those responsibilities.

[3] 47 U.S.C. § 35.
[4] Exec. Order No. 10530, § 5(a), 19 Fed. Reg. 2709, 2711 (1954). *See also* 47 C.F.R. § 1.767(b).
[5] *See*, *e.g.*, *Actions Taken Under Cable Landing License Act*, 34 FCC Rcd 8628 (2019), 32 FCC Rcd 3791, 3792-93 (2017), 28 FCC Rcd 1323, 1324 (2013), 24 FCC Rcd 2219, 2220 (2009), 23 FCC Rcd 13149, 13420 (2008).

Accordingly, NTIA on behalf of the Committee advises the Commission that the Committee has no objection to the Commission granting the above-captioned application, provided that the Commission conditions its consent on compliance with the July 6, 2020 NSA attached to this filing.

Respectfully submitted,

Kathy Smith
Chief Counsel

National Telecommunications and
Information Administration
1401 Constitution Avenue, NW
Washington DC 20230
(202) 482-1816

July 10, 2020

NATIONAL SECURITY AGREEMENT

This National Security Agreement (the "Agreement" or "NSA") is made as of the date of the last signature affixed hereto, by and between GU Holdings Inc. ("Google"), RTI JGA Pte. Ltd ("RTI JGA"), and RTI Connectivity Pte. Ltd. ("RTI Connectivity") (together with RTI JGA, "RTI"), and AARNet Pty Ltd. ("APL") (collectively, the "Licensees") on the one hand, and the U.S. Department of Homeland Security ("DHS"), the U.S. Department of Justice ("DOJ"), and U.S. Department of Defense ("DOD") (collectively "Government Parties" or "Compliance Monitoring Agencies" ("CMAs")) on the other hand (each referred to individually as a "Party" and collectively as the "Parties").

RECITALS

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, 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., Executive Order 13231, Critical Infrastructure Protection in the Information Age, and Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience);

WHEREAS, the Licensees seek to land and operate within the United States a private fiber-optic submarine cable network connecting Guam and Australia, called the Japan-Guam-Australia South System ("JGA-S");

WHEREAS, on June 21, 2019, the Licensees applied to the Federal Communications Commission ("FCC") for a submarine cable landing license under the Cable Landing License Act of 1921 and Executive Order No. 10530, FCC File No. SCL-LIC-20190502-00016 (the "Application");

WHEREAS, on June 25, 2019, DHS requested that the FCC defer action on the Licensees' application and remove it from streamline given that DHS was reviewing the matter for national security, law enforcement, and public safety issues, consistent with the consideration of such issues by the informal working group known as Team Telecom in TT # 19-025; and

WHEREAS, the Licensees have agreed to enter into this Agreement with the CMAs solely as a condition to the Application, and the Licensees understand that the CMAs will petition the FCC to condition its grant of the Application on compliance with this Agreement.

ARTICLE 1: DEFINITIONS

A. "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,.

B. "Domestic Communications Infrastructure" or "DCI" means: (a) any portion of JGA-S that physically is located in the United States, up to and including the submarine line terminating equipment, 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.*, Microsoft Office) used to provide, process, direct, control, supervise, or manage Domestic Communications; and (b) Network Operations Center ("NOC") facilities, as defined in Section I.E. below.

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

D. "Managed Service Provider" or "MSP" means any third-party that performs services to the Licensees in support of JGA-S's network operation, provision of services, management, production network, Domestic Communications, or DCI including, but not limited to, customer support, Operations Support Systems or Business Support Systems, maintenance, network operations center, information technology, cloud operations, and data center operations, but not including commercial off the shelf products.

E. "Network Operations Center" or "NOC" means the locations and facilities designated as such by the Licensees for purposes of performing network management, monitoring, maintenance, or other operational functions for JGA-S.

F. "Principal Equipment" means the primary electronic components of JGA-S, which includes the DCI and Wet Infrastructure. Principal Equipment consists of: network element servers; routers; switches; repeaters; submarine line terminal equipment ("SLTE"); system supervisory equipment ("SSE"); signal modulators and amplifiers; power feed equipment ("PFE"); tilt and shape equalizer units ("TEQ/SEQ"); optical distribution frames ("ODF"); branching units ("BU"); synchronous optical network ("SONET"); synchronous digital hierarchy ("SDH"); wave division multiplexing ("WDM"); dense wave division multiplexing ("DWDM"); coarse wave division multiplexing ("CWDM"); or optical carrier network ("OCx") equipment, as applicable; any non-embedded software used for monitoring, administration, or provisioning of JGA-S (with the exception of COTS software used for common business functions, *e.g.*, Microsoft Office); and any other such equipment, whether physical or logical, that performs the functions of the equipment described in this definition that JGA-S may use in the normal course of business.

G. "Screened Personnel" has the meaning given it in Section IV.C. below.

H. "United States" ("U.S.") means the several States, districts, and territories of the United States.

I. "Wet Infrastructure" means hardware components installed and residing on the undersea portion of JGA-S, 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 JGA-S.

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

ARTICLE II. OPERATIONS

A. Cable System Information.

1. Within **45 days** of the execution of this NSA, and, thereafter, within **30 days** upon request by the CMAs, the Licensees agree to make available the following JGA-S information:

(a) network management information, including, as follows: (1) a network map that includes physical and logical topology; (2) network and telecommunications architecture descriptions and associated descriptions of 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, and main distribution facilities; (5) an organizational chart, to include specific reference to the names and positions of senior officials responsible for operations of JGA-S; (6) descriptions of interfaces and connections to JGA-S for service offload, disaster recovery, or administrative functions; and (7) a chart or charts, as needed, reflecting ownership interests in JGA-S, to include ownership interests held in JGA-S's owner(s), and the control rights over points of presence ("PoPs"), NOCs, and cable landing stations;

(b) a complete and current list of all contracts held by the Licensees or their designee(s) for the maintenance, repair, and security of JGA-S;

(c) a restoration plan for the Principal Equipment and the Wet Infrastructure for JGA-S; and

(d) subject to applicable law, a list of all JGA-S customers and the respective amount of capacity or analogous rights (e.g. fiber pair or spectrum allocation) provided on JGA-S.

B. Operational Requirements.

1. With respect to the operation of JGA-S:

(a) The Licensees will have the ability to promptly and effectively interrupt, in whole or in part, traffic to and from the United States, on JGA-S by disabling or disconnecting circuits at the U.S. cable landing station or at other locations within the United States; and

(b) The Licensees will configure all necessary systems to ensure they can suspend or interrupt the optical carrier signal or all of JGA-S within the DCI.

(c) If any Licensee is required to interrupt traffic to or from the United States as a result of lawful U.S. process, it will be permitted to disclose publicly that it was required to interrupt service in response to lawful U.S. process consistent with any limits on disclosure that may be imposed by such lawful U.S. process and without disclosing any of the content of such request.

2. Within **45 days** of the execution of this NSA, the Licensees will provide the CMAs notice of the proposed location or locations and, if not any of the Licensees, the controller, operator, or manager for, JGA-S's NOC or NOCs and PoPs. The CMAS will approve or disapprove the location or locations or the controller, operator, or manager within **60 days** of acknowledgement of receipt.

(a) The Licensees will notify the CMAs of any proposed change to JGA-S's NOC or PoP locations, to include the addition of new NOC or PoP locations and of any proposed change to the controller, operator, or manager for JGA-S's NOC or NOCs, at least **45 days** in advance of such proposed change. Any proposed or new NOC or PoP location will be subject to review and approval or disapproval by the CMAs within **60 days** of receipt.

C. Change in Services or Cable Operations. The Licensees anticipate using JGA-S for (a) their or their affiliates' own internal use and/or (b) offering wholesale, government and enterprise customers leased, indefeasible right-of-use for, or other non-ownership interests of capacity, spectrum or dark fibers on particularized terms and conditions pursuant to individualized negotiations. The Licensees agree to notify the CMAs in

writing at least **45 days** prior to implementing any changes to the nature of these services as offered to non-affiliate third-party customers of any of the Licensees. The Licensees agree to provide a detailed description of the proposed change including the terms, conditions, or entities involved in making the change to the communications services or operations.

ARTICLE III. PRINCIPAL EQUIPMENT AND MSPs

A. Definition Supplementation. At the sole discretion of the CMAs, the Licensees will supplement in writing the foregoing definitions of Principal Equipment or MSPs to address subsequent technological developments with submarine systems.

B. Initial List.

1. Within **45 days** of the execution of this Agreement, the Licensees will provide the CMAs with a list ("Initial List"), that identifies and emphasizes any changes from the July 26, 2019 list submitted to the CMAs:

   (a) all Principal Equipment and MSPs, including:

      (1) a description of each item or service and the functions supported;

      (2) each item's manufacturer or service's provider; and

      (3) the model and/or version number of any hardware or software; and

   (b) any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment or servicing MSP support.

2. The CMAs will approve or disapprove the Initial List within **60 days** of receipt.

   (a) If within the 60-day approval/disapproval period, the CMAs seek additional information from the Licensees, the approval/disapproval period shall be extended by the number of days that the CMAs awaited the requested information.

   (b) In the event of a disapproval from the CMAs, the Licensees will not initiate or expand the existing deployment or reliance on, and will not enhance the capabilities of, any Principal Equipment or MSPs of which CMAs have disapproved, and the Licensees will meet, confer, and otherwise attempt in good faith to resolve the CMAs' reason for disapproval. Until the CMAs' rationale for disapproval is resolved, the

Licensees will not upgrade, install, replace, or service any disapproved Principal Equipment without written authorization from the CMAs.

C. Modifications to Existing Principal Equipment, MSPs, and Vendors, Contractors, and Subcontractors for the Same.

1. The Licensees will provide the CMAs at least **45 days'** advance notice prior to:

   (a) any maintenance, repair, or replacement that would result in any modification to the quantum, function, configuration, operation, or location of existing Principal Equipment;

   (b) any change to the list of vendors, contractors, or subcontractors involved in providing, installing, operating, managing, repairing, or maintaining the Principal Equipment or MSPs; and

   (c) 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).

2. The 45 days' advance notice requirement of Section III.C.1. is waived for any maintenance, repair, or replacement that is undertaken in response to an unforeseen or uncontrollable event and that is necessary to ensure the continued operability of JGA-S; however, in such circumstances, the Licensees agree to provide advance notice to the CMAs of the modification, if practicable, and, if impracticable, the Licensees agree to provide notice within **10 days** after the maintenance, repair, or replacement. This notice will include a detailed description of the equipment replaced and the circumstances surrounding the need to replace the Principal Equipment without 45 days' advance notice.

3. The CMAs will have **60 days** to review and approve or disapprove any notice submitted pursuant to the process outlined above in Sections III.C. 1. and 2.

   (a) If within the 60-day approval/disapproval period, the CMAs seek additional information from the Licensees, the approval/disapproval period shall be extended by the number of days the CMAs awaited the requested information.

   (b) In the event of a disapproval from the CMAs, the Licensees will not initiate or expand the existing deployment or reliance on, and will not enhance the capabilities of, any Principal Equipment or MSPs of which the CMAs have disapproved, and the Licensees will to meet, confer, and otherwise attempt in good faith to resolve the CMAs' reason for

disapproval. Until the CMAs' rationale for disapproval is resolved, the Licensees will not initiate the notified change without written authorization from the CMAs.

(c) In the event of a disapproval from the CMAs of maintenance, repair, or replacement undertaken pursuant to Section III.C.2 for which no advance notice was provided, Licensees will, if directed by the CMAs, remove and replace any Principal Equipment or cease the service offering or support notified to and disapproved by the CMAs.

D. Equipment Testing. The Licensees agree to provide at least **45 days'** advance notice prior to initiating the testing of any new Principal Equipment connected to JGA-S by any vendor not already on the approved Principal Equipment List.

1. The CMAs will approve or disapprove the proposed testing within **60 days** of receipt of the notice. In the event of a disapproval by the CMAs, the Licensees will not initiate the notified testing and will meet, confer, and otherwise attempt in good faith to resolve the CMAs' concerns. Until the concerns are resolved, the Licensees will not test such new Principal Equipment without written authorization from the CMAs.

ARTICLE IV: ACCESS AND SECURITY

A. Measures to Prevent Improper Use and Unauthorized Logical and Remote Access.

1. The Licensees will take practicable measures to prevent unauthorized logical and remote access to JGA-S and to prevent any unlawful use or disclosure of information carried on the same. For purposes of this Section, "practicable measures," at a minimum, include effectuating compliance with all U.S. laws and regulations governing cybersecurity, information security, and privacy and will be measures consistent with best practices and guidelines, including but not limited to the Cybersecurity Framework of the National Institute of Standards and Technology ("NIST") and 27001 Series standards of the International Organization for Standardization. These 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 or third-parties with logical or remote access to the DCI.

2. The Licensees will take appropriate measures to protect and promote resiliency of JGA-S, including measures to ensure that security patches for systems and applications are up to date.

3. The Licensees will maintain or exceed security standards and best practices utilized within the U.S. telecommunications industry for maintenance of password systems and firewalls, non-destructive access logs, and periodic internal audits of network security and associated network devices.

B. Physical Security Measures.

1. The Licensees will take practicable measures to physically secure JGA-S, including the DCI.

2. The Licensees will screen appropriate persons in accordance with Section IV.C. below, and the Licensees will require that all persons who physically access the DCI are escorted at all times by Screened Personnel, as defined herein.

C. Screening of Personnel.

1. The Licensees agree to implement, either directly or through a vendor or service provider, a process to screen any existing or newly-hired personnel of the Licensees (or any personnel performing under an agreement or arrangement with any of the Licensees) in, at minimum, the following circumstances:

   (a) any person whose position could involve logical access to the DCI; and

   (b) all personnel charged with securing the DCI.

2. The Licensees' personnel screening process will be reflected in a written policy subject to Section IV.D. of this Agreement and will include background investigations, public criminal records checks, or other analogous means to ascertain a person's trustworthiness. Upon satisfactory completion of the requirements set forth in the screening policy, such persons will be considered "Screened Personnel."

D. Security Policies. The Licensees will develop and implement one or more security policies that address the requirements of this Section ("Security Policies").

1. The Security Policies will be subject to review and approval by the CMAs, and the Licensees will submit their Security Policies to the CMAs within **90 days** of the date of execution of this Agreement. Within **105 days** of receipt, the CMAs will approve or disapprove the Security Policies. The Licensees will amend the Security Policies to the CMAs' satisfaction.

   (a) Changes to the Security Policies will be subject to review and approval by the CMAs.

(b) If within the 105-day approval/disapproval period, the CMAs seek additional information from the Licensees, the approval/disapproval period shall be extended by the number of days the CMAs awaited the requested information.

2. The Licensees will ensure that personnel are trained on and have access to the Security Policies, and the Licensees will take all necessary measures to facilitate full compliance by personnel with the Security Policies.

E. Reporting Incidents and Breaches.

1. The Licensees will report to the CMAs in writing within **48 hours** of learning information that reasonably indicates:

(a) unauthorized third-party access to, or disruption or corruption of, JGA-S or any information being carried on JGA-S;

(b) any other unauthorized access to or disclosure of Domestic Communications in violation of federal, state, or local law; or

(c) any material breach of the commitments made in this NSA.

2. The Licensees will submit in writing a follow-up report describing in greater detail any incident requiring notice pursuant to this Section and the Licensees steps to remediate that incident to the CMAs within **15 days** of discovery of the relevant conduct. The Licensees will also submit in writing supplementary information regarding any follow-up report until such evaluation is complete.

3. The Licensees will remediate any incidents or breaches reported pursuant to this Section to the satisfaction of the CMAs.

F. Instruction of Obligations. The Licensee will instruct appropriate officers, employees, contractors, and agents as to the Licensees' obligations under this NSA, including the individuals' duty to report any violation, and will issue periodic reminders of such obligations. The Licensees will issue initial instructions in writing and provide appropriate live training within **90 days** of the date of execution of this Agreement, and the Licensees will submit a copy of their written instructions to the CMAs at the same time. The Licensees will issue updated instructions or training annually thereafter.

ARTICLE V: OVERSIGHT

A. Change in Control. If any of the Licensees learns of any information that reasonably indicates that any foreign entity or individual, other than those already identified, has or likely will obtain an ownership interest, whether direct or indirect, in Google, RTI, APL, or JGA-S 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 Google, RTI or APL, the Licensees agree to provide notice in writing to the CMAs within **15 days**. Notice under this Section will, at a minimum:

1. identify the entity or individual(s) acquiring control (specifying the name, addresses, and telephone numbers of the entity or individual(s));

2. identify the beneficial owners of any such increased or prospective increased ownership interest in Google, RTI, APL, or JGA-S by the entity or individual(s) (specifying the name, addresses, and telephone numbers of each beneficial owner); and

3. quantify the amount of ownership interest that the entity or individual(s) has or likely will obtain in Google, RTI, APL, or JGA-S and, if applicable, the basis for their prospective control of Google, RTI, APL, or JGA-S.

B. Bankruptcy. The Licensees will provide the CMAs notice no later than **30 days** after initiating any bankruptcy proceeding or any other legal proceeding undertaken for the purpose of reorganizing, refinancing, or otherwise seeking relief from all or some of a Licensee's debts in relation to JGA-S.

C. Security Point of Contact.

1. Google will maintain a primary Point of Contact ("Primary POC") for purposes of this Agreement. RTI and APL will each maintain a secondary Point of Contact ("Secondary POC") for purposes of this Agreement. The Primary POC will be a U.S. citizen and be able to hold and maintain a U.S. Government security clearance at the "Secret" level or higher. The Primary POC will possess the appropriate authority, reporting lines, independence, skills, and resources to ensure compliance with the terms of this NSA.

2. Google, RTI, and APL will nominate a proposed Primary POC and Secondary POCs respectively within **45 days** of the execution of this Agreement. Within **60 days** of receipt of the nominations, the Primary POC and Secondary POCs will be subject to the CMAs' review and approval, including the nominees being subject to a background check at the sole discretion of the CMAs.

(a) Along with the name of any nominee for Primary POC and Secondary POCs, Google, RTI, and APL will provide the following information: (i) a curriculum vitae or similar professional synopsis; (ii) date of birth; (iii) place of birth; (iv) social security number; (iv) relevant contact information, including office and cell phone numbers, email, and emergency contact information; (v) residency address; and (vi) any other information identified by the CMAs as necessary for such nominees to ensure the nominee can effectively perform the functions set forth in this Agreement.

(b) In the event of a disapproval from the CMAs to a Primary POC or Secondary POC nomination, Google, RTI, or APL will submit a new nominee within **45 days** of the CMAs' disapproval, subject to the same terms as the original nomination pursuant to this Section.

3. Following approval of the Primary POC by the CMAs, Google will notify the CMAs at least **45 days** in advance of the Primary POC changing his or her residency to move more than 40 miles from the location most recently notified to the CMAs, and the CMAs may, in their sole discretion, disapprove of the residency change and notify Google that the proposed residency change disqualifies the Primary POC from continuing to serve in that position. If the CMAs disapprove of the residency change, Google shall nominate an alternative candidate within **15 days** of its receipt of any such disapproval, subject to the same review and approval procedures as the initial nomination.

4. The Primary POC will be available 24 hours per day, 7 days per week, regarding any national security, law enforcement, or public safety concerns that the CMAs may raise with respect to JGA-S. Upon request by the CMAs, the Primary POC or Secondary POCs will make himself/herself available in person within the United States within **5 days**, at a date and location, including in a classified setting, as deemed necessary by the CMAs. The Primary POC will be responsible for receiving and promptly effectuating any lawful inquiries or requests for information and for otherwise ensuring compliance with obligations set forth in this NSA. In the event a lawful inquiry or request for information implicates SLTE owned and/or operated by RTI or APL, the Primary POC will provide prompt notice of such inquiry or request to the relevant Secondary POC, who will promptly respond directly to the relevant government agency.

5. Google, RTI, and APL will notify the CMAs of any proposed change to the Primary POC or Secondary POCs at least **15 days** in advance of such proposed change (except in the case of the unexpected firing, resignation or death of the Primary POC or a Secondary POC in which case such written notice must be provided within **5 days** of such event). Google, RTI, and APL must nominate any

proposed Primary POC and Secondary POC, and any such nomination will be subject to the CMAs' review and approval in accordance with the procedures outlined in Section V.C.2.

D. Annual Report. On the anniversary of the date of this NSA, the Licensees agree to submit to the CMAs a report assessing the Licensees' compliance with the terms of this NSA for the preceding year. The CMAs may request specific content be included in a given year's Annual Report, but at a minimum, the report will include:

1. the names and contact information of the then-current Primary and Secondary POCs;

2. Cable System Information, as described in Section II.A. above, noting any changes during the reporting period;

3. a list identifying all of the current Principal Equipment and MSPs, as well as the vendors, contractors, or subcontractors involved in providing, installing, operating, managing, repairing, or maintaining the Principal Equipment or MSPs, containing all information described in Section III.B.1., identifying any material modifications during the reporting period;

4. a copy of the then-current Security Policies, and a summary of any changes during the reporting period and the reasons therefore;

5. a summary of any events that occurred during the reporting period that, to the knowledge of the Licensees, will or reasonably could impact the effectiveness of or compliance with this NSA; and

6. 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. Third-Party Audit. At their sole discretion, but no more frequently 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 the Licensees' compliance with the terms of this NSA.

1. The auditor will be subject to the CMAs' approval. Within **60 days** of the CMAs requesting a third-party audit, the Licensees will nominate 2 third-party auditor firms to the CMAs. Within **75 days** of the nominations, the CMAs will approve or disapprove the nominated third-party auditor firms.

(a) The Licensees may select any auditor approved by the CMAs.

(b) If the CMAs disapprove of either of the nominated third-party auditors, the Licensees 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, the Licensees will provide to the CMAs 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 the Licensees providing information regarding the Licensees' and the nominated auditor's pre-existing relationship (if any).

2. The Licensees will be solely responsible for any costs associated with any third-party audit carried out pursuant to this Section V.E. The CMAs will consider avoidance of unreasonable costs as a factor when exercising their rights under this Section.

3. The Licensees 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.

4. The Licensees will ensure that the complete, executed engagement agreement and all compensation terms with the third-party auditor related to the audit are provided to the CMAs within **5 days** of execution.

5. The third-party auditor will promptly deliver to the CMAs and Licensees all reports and related information generated or gathered during its review that relate directly to the Licensees' compliance with the terms of this NSA, and will meet independently with the CMAs upon request.

F. Consultation and Visitation by the CMAs.

1. The Licensees will produce requested documents to, and meet and confer with, the CMAs and resolve to the satisfaction of the CMAs any concerns the CMAs may raise regarding compliance with this NSA.

2. The Licensees will negotiate in good faith to resolve to the satisfaction of the CMAs any national security, law enforcement, or public safety concerns the CMAs may raise with respect to any matters set forth in this NSA.

3. Upon 48 hours advance notice, except when due to exigent circumstances advance notice is not practicable, the CMAs may visit JGA-S facilities and any facility that is or has been used for discharging the Licensees' obligations under this NSA to conduct on-site reviews solely to verify the implementation of and compliance with the terms of this NSA. Subject to applicable law and consistent with security requirements, during such visits, the Licensees will cooperate for these purposes and provide 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, Licensees shall provide the CMAs with access to information, facilities and personnel within 24 hours of such an access request.

ARTICLE VI: GENERAL PROVISIONS

A. Successors and Assigns. This NSA shall inure to the benefit of, and shall be binding upon, the Licensees and their successors, assigns, subsidiaries, and affiliates; for purposes of this Agreement, successors and assigns shall include any corporate name changes. The Licensees will not assign any obligation under this NSA without the prior written consent of the CMAs, and the Licensees will remain responsible for the activities of any person to whom they assign any obligation under this Agreement.

B. Breach. Each Licensee agrees that, in the event that a Licensee 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 CMAs may request that the FCC modify, condition, revoke, cancel, terminate, or render null and void the license granted by the FCC for the landing and operation of JGA-S, in addition to any other remedy available at law or equity.

C. Individual Responsibility. The CMAs acknowledge there can be instances in which the individual Licensees obligations will not extend to the obligations or conduct of other Licensees.

D. Changed Circumstances. If, after this NSA takes effect, the CMAs or any of the Licensees believe that changed circumstances warrant modifying or terminating this NSA (including if the CMAs determine that the terms of this NSA are inadequate or no longer necessary to address national security, law enforcement, or public safety concerns), the Licensees and CMAs agree to negotiate in good faith to modify this NSA. Rejection of a proposed modification alone shall not constitute evidence of a failure to negotiate in good

faith. Modification or termination of this Agreement must be executed by written agreement signed by the Parties.

E. Choice of Law. This Agreement shall be governed by and interpreted according to the Federal laws of the United States.

F. Compliance with Applicable Law. Nothing in this NSA excuses the Licensees from their obligations to comply with any and all applicable legal requirements and obligations, including all applicable statutes, regulations, requirements, or orders.

G. Computing Time. In computing any time period pursuant to this Agreement, the below rules apply.

1. For any period stated in days:

   (a) the day of the event that triggers the period is excluded;

   (b) every day thereafter is counted, including intermediate Saturdays, Sundays, and federal holidays, except for those days that are tolled pursuant to Section VI.G.3.; and

   (c) the last day of the period is included, but if the last day is a Saturday, Sunday, or federal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or federal holiday.

2. For any period stated in hours:

   (a) begin counting immediately on the occurrence of the event that triggers the period;

   (b) count every hour, including hours during intermediate Saturdays, Sundays, and federal holidays, except for those hours that are tolled pursuant to Section VI.G.3.; and

   (c) if the period would end on a Saturday, Sunday, or federal holiday, the period continues to run until the same time on the next day that is not a Saturday, Sunday, or federal holiday.

3. Any approval provision applicable to the CMAs pursuant to this Agreement shall be tolled during a lapse in appropriations or any time when the Federal government in the greater Washington, D.C. area is closed.

H. Notices. All notices and other communications given or made relating to this NSA shall be (i) in writing; (ii) sent by electronic mail 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; and (iii) deemed to have been duly given or made as of the date of receipt of such electronic mail:

If to the CMAs:

U.S. Department of Defense
Attention: Barbara M. Key
Risk Management and Operational Integration
6000 Defense
Pentagon, Rm 3D253
Washington, DC 20301-6000
osd.pentagon.dod-cio.list.team-telecom@mail.mil

U.S. Department of Homeland Security
Attention: Alton O. Turner
Office of Strategy, Policy, and Plans
Foreign Investment Risk Management (FIRM)
Mail Stop 0445
2707 Martin Luther King Avenue, SW
Washington, DC 20528
Compliance@hq.dhs.gov
IP-FCC@hq.dhs.gov

U.S. Department of Justice
Foreign Investment Review Section
Attention: Eric S. Johnson
175 N Street, NE
12th Floor
Washington, DC 20530
Compliance.telecom@usdoj.gov

If to GU Holdings:

GU Holdings Inc.
c/o Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043 USA
Attn: General Counsel
Facsimile: (650) 618-1833

Email: legal-notices@google.com

If to RTI:

Grace Guang
General Counsel
RTI Group
268 Bush Street #77
San Francisco, California 94104
grace.guang@rticable.com

with a copy to:

Kent Bressie
Harris, Wiltshire & Grannis LLP
1919 M Street, N.W., Suite 800
Washington, D.C. 20036-3537
kbressie@hwglaw.com

If to APL:

AARNet Pty Ltd
Mary Fleming
Level 7 Tower A, 799 Pacific Highway
Chatswood NSW 2067
Australia
mary.fleming@aarnet.edu.au

I. Point of Contact for the CMAs Regarding Legal Matters. If represented by legal counsel as regards to compliance with this Agreement, the Licensees will identify to the CMAs the contact information for one or more such counsel, whether outside legal counsel or internal counsel, within **10 days** of the date of the NSA's execution and thereafter shall keep such legal contact information up to date with the CMAs.

J. Direct Communications. The Licensees acknowledge that the CMAs may communicate directly with the Primary POC, Secondary POCs, Auditor and his/her staff, and any other point of contact designated by the Licensees. The Licensees further acknowledge that the CMAs may communicate directly with any personnel from Google, RTI, or APL who initiate or are included on communications with the CMAs regarding the NSA. These acknowledgments shall in no way prohibit or otherwise inhibit any of the Licensees from consulting with, obtaining advice from, or communicating with the CMAs through counsel.

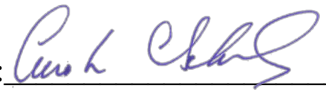
K. Severability. The provisions of this Agreement shall be severable and if any provision hereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of such other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

L. Effectiveness of Agreement. Except as otherwise specifically provided in the provisions of this Agreement, the obligations imposed and rights conferred by this Agreement shall take effect upon the date this Agreement is signed by the last Party to sign it.

M. Waiver. The failure of the CMAs to insist on strict performance of any of the provisions of this Agreement, or to exercise any right granted herein, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by the CMAs of any provision of, or right under, this Agreement shall be valid unless it is in writing and expressly provides for the waiver of a specified requirement under a particular provision of this Agreement.

[Remainder of page intentionally left blank]

GU Holdings Inc.

By: 
Name: Austin Schlick
Title: President
Date: July 3, 2020

RTI JGA Pte. Ltd.

By:_____
Name:
Title:
Date:

RTI Connectivity Pte. Ltd.

By:_____
Name:
Title:
Date:

AARNet Pty Ltd.

By:_____
Name:
Title:
Date:

GU Holdings Inc.

By:_____
Name: Austin Schlick
Title: President
Date:

RTI JGA Pte. Ltd.

By:_____
Name: Kam Kian Kok
Title: Director
Date: July 2, 2020

RTI Connectivity Pte. Ltd.

By:_____
Name: Russell Matulich
Title: Chief Executive Officer
Date: July 2, 2020

AARNet Pty Ltd.

By:_____
Name:
Title:
Date:

GU Holdings Inc.

By:_____
Name: Austin Schlick
Title: President
Date:

RTI JGA Pte. Ltd.

By:_____
Name:
Title:
Date:

RTI Connectivity Pte. Ltd.

By:_____
Name:
Title:
Date:

AARNet Pty Ltd.

By:_____
Name: M E FLEMING
Title: DIRECTOR INTERNATIONAL
Date: 4 July 2020

For the U.S. Department of Homeland Security

By: _____
Name: Scott Glabe
Title: Assistant Secretary for Trade and Economic Security
Office of Strategy, Policy, and Plans
Date: 7/2/20

For the U.S. Department of Justice

By: _____
Name:
Title:
Date:

For the U.S. Department of Defense

By: _____
Name:
Title:
Date:

For the U.S. Department of Homeland Security

By:_____
Name:
Title:
Date:

For the U.S. Department of Justice

By:_____
Name: Eric S. Johnson
Title: Deputy Chief, National Security Division
Date: 7/6/20

For the U.S. Department of Defense

By:_____
Name:
Title:
Date:

For the U.S. Department of Homeland Security

By:_____
Name:
Title:
Date:

For the U.S. Department of Justice

By:_____
Name:
Title:
Date:

For the U.S. Department of Defense

By: _____
Name: John W. Wilmer
Title: Deputy CIO, Cybersecurity
Date: 07/06/2020