NATIONAL SECURITY AGREEMENT

This National Security Agreement (the "Agreement" or "NSA") is made as of the date of the last signature affixed hereto ("Effective Date"), by and between Quintillion Subsea Operations, LLC ("QSO"), Q Gateway Ultimate Holdings, LLC ("Q Gateway"), and Grain Communications Opportunity Fund III, Master, L.P. ("GCO III") (together, the "Parties"), on one hand, and, on the other, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Committee"), represented by the U.S. Department of Homeland Security ("DHS"), the U.S. Department of Justice ("DOJ"), and the U.S. Department of Defense ("DOD") (collectively, the "Compliance Monitoring Agencies" or "CMAs) (each referred to individually as a "Signatory" and collectively as " Signatories").

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, 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, Executive Order 13231, as amended; and Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience);

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, Executive Order 13873, 84 Fed. Reg. 22,689 (May 15, 2019);

WHEREAS, on March 27, 2017, the FCC authorized QSO to construct, land, and operate a multi-stage high-capacity fiber optic cable system extending between Nome, Alaska and Prudhoe Bay, Alaska, the Quintillion Cable System ("Quintillion"), FCC File No. SCL-LIC-20160325-00009 ("License");

WHEREAS, the License was granted by the FCC conditioned on compliance with a Letter of Assurances ("LOA") dated March 24, 2017 executed by QSO to the CMAs;

WHEREAS, on May 26, 2021, QSO, at the request of CMAs, agreed to enter in an NSA to address national security, law enforcement, and public safety concerns raised with regard to an application filed by QSO with the FCC (File No. SCL-LIC-20160325-00009) requesting authority to construct, land, and operate Quintillion;

WHEREAS, the Committee has undertaken a review of the Application[1] pursuant to Executive Order 13913, 85 Fed. Reg. 19643 (Apr. 8, 2020), to evaluate whether granting the consent to transfer control of Quintillion and the License for Quintillion from QSO and QSH Parent Holdco, LLC to Q Gateway may pose a risk to the national security and law enforcement interests of the United States;

WHEREAS, the Committee has determined, based on a risk-based analysis, as required by Executive Order 13913 Section 9(c), that it is necessary to enter into this NSA with the Parties to mitigate risk to U.S. national security and law enforcement interests raised by the Application;

WHEREAS, the Parties certify as true and correct, under penalties outlined in 18 U.S.C. § 1001, all statements the Parties or their representatives have made to DHS; DOJ, including the Federal Bureau of Investigation; DoD; and the FCC in the course of the review of the Application that the Committee conducted pursuant to Executive Order 13913;

WHEREAS, the Signatories hereby adopt those statements as the basis for this NSA;

WHEREAS, the Signatories have agreed and understand that upon execution of this NSA, the Committee will petition the FCC to condition the transfer of the License on the Parties' compliance with this NSA; and

WHEREAS, this NSA will supersede and replace in its entirety the LOA executed on March 24, 2017 and the NSA executed on May 26, 2021.

ARTICLE I

DEFINITION OF TERMS

1.1 Definitions. As used in this NSA, capitalized terms shall be defined as set forth below; *provided that* capitalized terms used in these conditions and not defined in this Article I shall have the meanings assigned to them elsewhere in this Agreement.

(a) "Access" means to, or the right or ability to, enter a location or physical space; or 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

[1] FCC File No. SCL-T/C 20230411-00010 (TT 23-030).

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). As used in this Agreement, Access should be construed broadly to include rather than exclude conduct.

(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 Quintillion and that requires response and recovery.

(c) "Domestic Communications" means: (i) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location and (ii) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States or its territories.

(d) "Domestic Communications Infrastructure" or "DCI" means: (i) any portion of Quintillion that physically is located in the United States or its territories, up to and including the submarine line terminating 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.*, Microsoft Office) used by or on behalf of the Parties to provide, process, direct, control, supervise, or manage Domestic Communications; and (ii) Network Operations Center ("NOC") facilities, as defined below.

(e) "Electronic Communication" has the meaning set forth in 18 U.S.C. § 2510(12).

(f) "Internet Protocol Detail Record" or "IPDR" means information about internet protocol-based usage and other activities that can be used by operation support systems and business systems by recording data statistics that provide network insight on capacity, subscriber usage, and proactive network maintenance.

(g) "Network Operations Center" or "NOC" means the locations and facilities designated as such by the Parties for purposes of performing network management, monitoring, maintenance, or other operational functions for Quintillion.

(h) "Personally Identifiable Information" or "PII" means any information that uniquely identifies and correlates to a natural person or can be used to distinguish or trace a natural person's identity alone, including a natural person's name, social security number, or biometric records, or when combined with other personal or identifying information that is linked or linkable to a specific individual, including date and place of birth, or parent's surname.

(i) "Principal Equipment" means the primary electronic components of Quintillion that support the subsea cable system end-to-end. This term includes the DCI and Wet Infrastructure/Plant. Principal Equipment also includes, but is not limited to: network element servers; routers; switches; repeaters; SLTE, including but not limited to SLTE that the Parties own or lease and SLTE owned or operated by other entities that hold capacity on Quintillion;

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; all software used to support, monitor, or administer Quintillion operations and services (with the exception of COTS software used for common business functions, *e.g.*, Microsoft Office); and 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 Quintillion, or which the Parties have definitive plans to employ or otherwise use on Quintillion.

(j) "Screened Personnel" has the meaning set forth in Article 5.3 below.

(k) "Security" means a condition that results from the establishment and maintenance of protective measures that enable 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.

(l) "Sensitive Personal Data" has the meaning set forth in 31 C.F.R. § 800.241.

(m) "Subscriber Information" means any information of the type referred to and accessible subject to the procedures set forth in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

(n) "U.S. Records" means the Parties' customer billing records, Subscriber Information, PII, Sensitive Personal Data, IPDRs, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by the Parties in connection with Quintillion within the United States, 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.

(o) "Wet Infrastructure" or "Wet Plant" means hardware components installed and residing on the undersea portion of Quintillion, including fiber optic cables, repeaters, BUs, and routers (if any). Wet Infrastructure includes all the components used to define the topology of the undersea portion of Quintillion.

(p) "Wire Communication" has the meaning set forth in 18 U.S.C. § 2510(1).

ARTICLE II

SECURITY OFFICER

2.1 The Parties agree QSO will appoint and maintain a Security Officer who is responsible for overseeing compliance with this NSA. The Security Officer will be a U.S. citizen who, to the knowledge of QSO, is eligible for a U.S. government security clearance at the "Secret" level or higher. The Security Officer will possess the appropriate senior-level corporate

authority, reporting lines, independence, technical skills, and resources required to assess the physical and logical security of subsea cable systems and to ensure compliance with the terms of this NSA. The Security Officer will have access to all records, information technology ("IT") networks, and personnel necessary to fulfill his or her duties pursuant to this NSA.

2.2 QSO agrees to nominate a proposed Security Officer within **30 days** of the execution of this NSA. QSO understands that the Security Officer nomination will be subject to CMA review and approval and may be subject to a background check at the sole discretion of the CMAs. In order to facilitate this, QSO will provide the CMAs with the Security Officer's PII, contact information, and any other information requested by the CMAs, at the time of nomination and in a format that the CMAs will identify.

2.3 The CMAs will approve or disapprove the proposed Security Officer within **30 days** of receiving the nomination. If the CMAs approve the nominee, QSO will appoint the Security Officer to this position within **3 days** following the CMAs' approval. If the CMAs disapprove the Security Officer nominee, QSO will nominate a different candidate within **30 days** following the receipt of such disapproval. QSO agrees to notify the CMAs of any proposed change to the Security Officer at least **15 days** in advance of such proposed change (except in the cases of an unexpected firing, resignation, or death of a Security Officer, in which cases such written notice must be provided within **5 days** of such event). For avoidance of doubt, QSO shall not remove the Security Officer for any reason arising from the Security Officer's attempts to comply with or ensure the Parties' compliance with this NSA. QSO understands that any proposed Security Officer nomination will be subject to CMA review and approval pursuant to this Article as outlined above.

2.4 The Security Officer will be available **24 hours** per day, **7 days** per week, to respond to any national security or law enforcement concerns that the CMAs may raise with respect to Quintillion. Upon request from the CMAs, the Security Officer will be available in person within the United States at a mutually agreeable date and location within **72 hours** of such request, including in a classified setting as necessary. The Security Officer will be responsible for receiving and promptly effectuating any lawful inquiries or requests for information and for otherwise ensuring compliance with all obligations set forth in this NSA.

ARTICLE III

OPERATIONS AND FACILITIES

3.1 Cable System Information. Within **30 days** of the execution of this NSA, and, thereafter, within **30 days** upon the CMAs' request, the Parties agree to make available the following Quintillion Cable System Information:

(a) Network management information, including: (1) a network map that includes physical and logical topology, including any terrestrial backhaul from the cable landing stations to the SLTE locations or other facilities housing Quintillion Principal Equipment; (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 Party officials responsible for operations of Quintillion, and/or senior officials of any third parties performing such duties on behalf of the Parties; and (6) descriptions of interfaces and connections to Quintillion for service offload, disaster recovery, or administrative functions;

(b) A complete and current list of all contracts held by the Parties or their designee(s) for the maintenance, repair, and Security of Quintillion;

(c) A restoration plan for the Principal Equipment and the Wet Infrastructure for Quintillion;

(d) A complete and current list of all entities, excluding the Parties, that hold capacity on Quintillion and own or operate SLTE for Quintillion; and

(e) A complete and current list of all entities, excluding the Parties, that hold capacity on Quintillion and have logical or physical Access to Quintillion Principal Equipment.

3.2 Operational Requirements

(a) With respect to the operation of Quintillion, the Parties agree as follows:

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

(ii) The Parties will configure all necessary systems to ensure the NOC can suspend or interrupt the optical signal or all communications functionality of Quintillion; and

(iii) If the Parties are required to interrupt traffic to or from the United States as a result of lawful U.S. process, the Parties will be permitted to disclose publicly that they were 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 other content of such request.

(b) Within **30 days** of the execution of this NSA, the Parties will submit to the CMAs the NOC location(s) with the controller, operator, or manager for the NOC(s) for CMA approval. The CMAs will approve or disapprove the locations and operators within **45 days** of receipt. The Parties agree to notify the CMAs of any proposed change to NOC location(s) or operator(s), to include the addition of new NOC locations, at least **45 days** in advance of such proposed change. The Parties understand the CMAs will approve or disapprove the new operator, location, or locations within **45 days** of acknowledgement of receipt.

3.3 Change in Services or Cable Operations

(a) The Parties agree to notify the CMAs in writing at least **30 days** prior to implementing any changes to the operations of Quintillion as they previously have been disclosed in writing to the CMAs pursuant to this NSA. The Parties agree to provide a detailed description of any such proposed change including the terms, conditions, individuals, and/or entities involved in making the change to the operations of Quintillion.

(b) The Parties further agree to notify the CMAs in writing at least **30 days** prior to the start of construction of a new BU or change in system topology. Upon request, the Parties will provide quarterly updates to the CMAs regarding the status of any notified expansion plans under Article 3.1, on a schedule approved by the CMAs.

(c) The Parties will notify the CMAs in writing within **5 days** of any filing of an application with the FCC for approval regarding any additional landing points for Quintillion or any modification application.

ARTICLE IV

PRINCIPAL EQUIPMENT, VENDORS, AND CONTRACTORS

4.1 Principal Equipment

(a) Within **30 days** of the execution of this NSA, the Parties agree to provide the CMAs with a list ("Principal Equipment List") to include the following information in a format that the CMAs will identify:

(i) A complete and current Principal Equipment List, including the following:

(1) Manufacturer Information

(A) Name

(B) Business Address

(C) Employer Identification Number ("EIN")[2]

(D) Webpage Address URL; and

(2) Equipment Information

(A) Make

(B) Model/Version Number

(C) Function of Item

[2] The Parties shall provide such information to the extent it is known and available.

(D) Country Where Item Is Located

(E) Owner of Item (including, for example, if rented or owned by an entity holding capacity on Quintillion).

(ii) The name, address, phone numbers, and website for any vendors, contractors, subcontractors, or other entities, including entities that hold capacity on Quintillion, involved in providing, installing, operating, managing, repairing, analyzing, securing, monitoring, or maintaining the Principal Equipment.

(b) CMA objections to the Principal Equipment List will be handled pursuant to Article 4.5.

(c) At the sole discretion of the CMAs, the Parties agree to supplement in writing the foregoing definition of Principal Equipment to address subsequent technological developments with submarine systems.

4.2 Modifications to Existing Principal Equipment

(a) The Parties agree to provide the CMAs at least **30 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 existing Principal Equipment.

(b) The Parties agree to receive CMA approval prior to the addition of any sensing technology (such as distributed acoustic, thermal, seismic, or other sensing technologies) to Quintillion.

(c) The CMAs will approve or disapprove any such modifications pursuant to Article 4.5.

(d) For any maintenance, repair, or replacement that would result in any modification to the quantum, function, configuration, operation, or location of existing Principal Equipment, and that is undertaken in response to an unforeseen or uncontrollable event and is necessary to ensure the continued operability of Quintillion, the Parties agree to provide advance notice to the CMAs of the modification, if practicable. Where providing advance notice is impracticable, the Parties will provide the CMAs with 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 beginning the maintenance, repair, or replacement.

(e) The Parties may continue to utilize any Principal Equipment maintained, repaired, or replaced pursuant to the process outlined in this Section, including in the case of unforeseen or uncontrollable events, provided that the CMAs do not object pursuant to Article 4.5.

4.3 Change in Vendors, Contractors, or Subcontractors for Principal Equipment

(a) The Parties agree to provide the CMAs with at least **30 days'** advance notice prior to any addition to the list of vendors, contractors, subcontractors, or other entities involved in providing, installing, operating, managing, repairing, analyzing, securing, monitoring, or maintaining the Principal Equipment for Quintillion.

(b) For any change that is undertaken in response to an unforeseen or uncontrollable event and is necessary to ensure the continued operability of Quintillion, the Parties agree to provide advance notice to the CMAs of such change, if practicable. Where providing advance notice is impracticable, the Parties will provide the CMAs with a detailed description of the change and the circumstances surrounding the need to conduct such activity without prior notice within **10 days** of such change.

(c) In addition, the Parties agree to provide the CMAs with at least **30 days'** advance notice prior to changing the service offerings or support from a previously listed vendor, contractor, subcontractor (*i.e.*, where a previously listed provider will be offering support in a previously unidentified way).

(d) Objections by the CMAs to any new vendor, contractor, or subcontractor for the Principal Equipment or the proposed service offerings thereof will be handled pursuant to Article 4.5.

4.4 Equipment Testing

(a) The Parties agree to provide the CMAs with at least **30 days'** advance notice prior to initiating the testing of any new Principal Equipment for Quintillion by any entity not already on the approved Principal Equipment List.

(b) The Parties agree to receive CMA approval prior to the testing of any sensing technology (such as acoustic, thermal, seismic, or other sensing technologies) on Quintillion.

(c) Objections by the CMAs to any testing proposed pursuant to this Section will be handled pursuant to Article 4.5.

4.5 Objection Resolution. Within **90 days** of receipt of any notice provided by the Parties pursuant to Articles 4.1, 4.2, 4.3, and 4.4, the CMAs will provide either written approval or disapproval to the Parties of the action described in such notice. If within the 90-day approval/disapproval period the CMAs seek additional information from the Parties, the approval/disapproval period shall be extended by the number of days the CMAs awaited the requested information. In the event of disapproval by the CMAs, the Parties will not expand the existing deployment or enhance the capabilities of any Principal Equipment of which the CMAs have disapproved, and the Parties agree to meet and confer with the CMAs and to resolve the CMAs' disapproval. Until the CMAs' disapproval is resolved, the Parties will not upgrade, install, replace, or service any disapproved Principal Equipment without written authorization from the CMAs.

ARTICLE V

USE, ACCESS, AND SECURITY

5.1 Measures to Prevent Improper Use and Unauthorized Access

(a) The Parties agree to take practicable measures to prevent unauthorized logical Access to Quintillion and to prevent any unlawful use or disclosure of information being carried on the cable. The Parties will include these measures in the policies that they will develop and implement pursuant to this NSA. For purposes of this Section, these measures shall, at a minimum, include policies and procedures to ensure compliance with all applicable U.S. laws and regulations governing cybersecurity, information security, and privacy and will be 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 measures should also include items such as (i) configuration management, (ii) security audits, (iii) system interconnection documentation, (iv) contractual safeguards, and (v) and screening procedures for personnel with logical Access to the DCI.

(b) The Parties agree to establish and maintain policies relating to Quintillion that will include, among other things, policies or plans relating to their 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, and protection of U.S. Records obtained by the Parties in the ordinary course of business. In accordance with Article 5.4(b), the policies will also include the Parties' plans regarding new contracts or amendments to existing contracts with third-party providers with Access to U.S. Records related to Quintillion that require those third parties to notify the Parties in the event of unauthorized Access to or disclosure 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.

(c) The Parties agree to take appropriate measures to protect and promote the resiliency of Quintillion, including measures to ensure that security patches for systems and applications are up to date.

(d) The Parties agree to 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 Quintillion, maintenance of non-destructive logical Access logs, and periodic internal audits of network security and associated network devices.

(e) The Parties agree to submit a policy regarding logical security measures adopted in accordance with the requirements of this Section to the CMAs within **90 days** of the execution of this NSA. Such policy will describe logical security measures and access controls adopted for both the common elements of Quintillion and for any separately-owned and operated equipment for Quintillion. The Parties agree that the policy will be updated when appropriate to conform with evolving information security standards and that the Parties will make additional

modifications to the policy, if requested by the CMAs, to address national security or law enforcement concerns, and work with the CMAs to implement such modifications. The CMAs will approve or disapprove the policy within **90 days** of receipt.

5.2 Physical Security Measures

(a) The Parties agree to take practicable measures to physically secure Quintillion, including the DCI and Wet Infrastructure. The Parties will screen appropriate personnel in accordance with Article 5.3 below, and the Parties will require that all persons who physically Access the DCI are escorted at all times by Screened Personnel, as defined in herein.

(b) The Parties agree to submit a policy setting forth their physical security measures to the CMAs within **90 days** of the date of the execution of this NSA. Such policy will describe physical security measures adopted for both the common elements of Quintillion and for any separately-owned or operated equipment for Quintillion. The CMAs will approve or disapprove the policy within **90 days** of receipt.

5.3 Screening of Personnel

(a) The Parties agree to implement, either directly (including through an affiliate) or through a vendor or service provider, a process to screen any existing or newly hired personnel (or any personnel performing under an agreement or arrangement with the Parties to do the same) in, at minimum, the following circumstances:

(i) Any person whose position could involve logical Access to the DCI, and

(ii) Any person charged with securing the DCI.

(b) The Parties personnel screening process will be reflected in a written policy ("Screening Policy") 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."

(c) The Parties will conduct background and criminal records checks on previously Screened Personnel every **7 years**.

(d) The Parties agree to submit the Screening Policy to the CMAs within **90 days** of the execution of this NSA. Such policy will describe the personnel screening process applicable to the common elements of Quintillion and to any separately-owned or operated equipment for Quintillion, including any separately-owned SLTE. The CMAs will approve or disapprove the policy within **90 days** of receipt. The Parties agree to cooperate with any request by the CMAs to provide additional identifying information regarding Screened Personnel.

(e) Within **45 days** of CMA approval of the Screening Policy, and with the annual report thereafter, the Parties agree to submit a list of all foreign Screened Personnel to the CMAs. Such list will include the following information in a format that the CMAs will identify:

(1) full name (last, first, middle name); (2) all other names and aliases used; (3) all countries of citizenship; (4) residence address; (5) work address; (6) country and city of residence; (7) date of birth; (8) place of birth; (9) U.S. social security number (where applicable); (10) national identity number, including nationality, date and place of issuance, and expiration date (where applicable); (11) U.S. or foreign passport number (if more than one, all must be fully disclosed); (12) systems and networks to which the individual has Access (if any); (13) type of Access (*i.e.*, read only, read/write); and (14) location from where the individual has such Access. The CMAs reserve the right to object to any person listed on the Screened Personnel list. In the event of any objection, the Parties agree to prohibit Access by the person or persons to whom the CMAs have objected.

5.4 Reporting Incidents and Breaches

(a) The Parties agree to report to the CMAs within **48 hours** if they learn of information that reasonably indicates:

(i) Unauthorized third-party Access to, or disruption or corruption of, Quintillion or any service or information being carried on Quintillion;

(ii) Any other unauthorized Access to or disclosure of Domestic Communications on Quintillion in violation of federal, state, or local law;

(iii) Any material breach of the commitments made in this NSA, including a violation of any approved plan, policy, or procedure under this NSA;

(iv) Any unauthorized Access to, or disclosure of, information obtained from or relating to government entities in connection with Quintillion; or

(v) Any one or more of the following which affect the Parties' computer network(s) or associated information systems in connection with Quintillion:

(1) Unauthorized disruptions to a service or denial of a service;

(2) Unauthorized processing or storage of data;

(3) Unauthorized modifications to system hardware, firmware, or software, including the identification of vulnerabilities introduced through a cyber supply chain compromise;

(4) Unplanned incidents that cause activation of the Parties' Cybersecurity Incident Response Plan;

(5) Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect the Parties' ability to comply with the terms of this NSA; or

(6) 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.

(b) The Parties agree to require any of their third-party service providers for Quintillion to disclose to the Parties any Security breach in connection with Quintillion, whether from data breach or other cause, within **72 hours** of the third party discovering the breach, unless the CMAs grant a waiver. The Parties further agree to require any of their third-party service providers for Quintillion to disclose to the Parties within **72 hours** of discovery, unless the CMAs grant a waiver, any critical exposure, threat, and vulnerabilities activating their Cybersecurity Incident Response Plan, associated with the products or services provided to the Parties including as a result of tainted software, introduction of malware, insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software and hardware, as well as poor development and manufacturing practices in the cyber supply chain.

(c) Upon the CMAs' request, the Parties agree to submit in writing a follow-up report describing in greater detail the incident or breach and the Parties' steps to remediate the incident or breach to the CMAs within **15 days** of discovery of the relevant conduct. The Parties also agree to submit in writing supplementary information regarding any follow-up report until such evaluation is complete. The Parties agree to remediate any incidents or breaches reported pursuant to this provision to the satisfaction of the CMAs.

5.5 Instructions of Obligations. The Parties agree to instruct appropriate officers, employees, contractors, and agents as to the Parties obligations under this NSA, including the individuals' duty to report any violation, and to issue periodic reminders of such obligations. The Parties agree to issue initial instructions in writing and provide appropriate live or virtual training within **90 days** of the execution of this NSA and the Parties agree to submit a copy of such instructions to the CMAs at the same time. The Parties agree to update and issue these instructions in writing and provide live or virtual training on annual basis.

ARTICLE VI

OVERSIGHT

6.1 Change in Control. If the Parties learn of any information that reasonably indicates that any single foreign entity or individual, other than those already identified, has or likely will obtain an ownership interest, whether direct or indirect, in the Parties or Quintillion 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, within the meaning of the definition sent forth in 47 C.F.R. § 63.09(b); or (ii) *de facto* or *de jure* control of the Parties or Quintillion, the Parties agree to provide written notice to the CMAs within **30 days**. The Parties also agree to provide the CMAs with written notice of any changes to the Parties' business(es) including not limited to (a) ultimate beneficial ownership changes; (b) corporate headquarter location changes; or (c) business operation location changes within **30 days** of such change. Notice under this Section will, at a minimum:

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

(b) Identify the beneficial owners of any such increased or prospective increased ownership interest in the Parties or Quintillion by the entity or individual(s) (specifying the name, addresses, and telephone numbers of each beneficial owner);

(c) Quantify the amount of ownership interest that the entity or individual(s) has or likely will obtain in the Parties or Quintillion and, if applicable, the basis for its prospective control of the Parties or Quintillion; and

(d) Other information relevant to the change or requested by the CMAs.

6.2 Bankruptcy. The Parties will provide the CMAs notice within **30 days** of 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 their debts.

6.3 Annual Report. On the anniversary of the date of execution of this NSA, the Parties agree to submit to the CMAs a report assessing the Parties' compliance with the terms of this NSA for the preceding year. The report shall include:

(a) The names and contact information of the Security Officer;

(b) Cable System Information, as described in Article 3.1 above, noting any changes during the reporting period;

(c) An updated Principal Equipment List for Quintillion containing all information described in Article 4.1 above, 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 (Article 5.1), physical security (Article 5.2), personnel screening (Article 5.3), incident reporting (Article 5.4), and employee training (Article 5.5), and a summary of any changes during the reporting period and the reasons therefor;

(e) An update regarding any expansion plans for Quintillion;

(f) An updated foreign Screened Personnel list (within the meaning of Article 5.3);

(g) Confirmation if the Parties have used in the past year, or plan to use in the future, logic-bearing (e.g., readable, writable, programmable) hardware, firmware, or software in their DCI, Principal Equipment, or other systems supporting DCI, Domestic Communications, or U.S. Records, that was designed, produced, or maintained by suppliers owned or controlled by, or subject to the jurisdiction or direction of, a U.S. Foreign Adversary (as designated by the Secretary of Commerce under Executive Order 13873 or any U.S. federal agency given subsequent comparable authority);

(h) Confirmation if the Parties have used in the past year, or plan to use in the future, products or services from an entity listed on the FCC's Covered List (see FCC, List of Equipment and Services Covered by Section 2 of the Secure Networks Act,

https://www.fcc.gov/supplychain/coveredlist)[3], the Commerce Department's Entity List, or subject to a removal or exclusion order issued by the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence pursuant to the SECURE Technology Act, 41 U.S.C. § 1321 et seq.;

(i) 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;

(j) 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; and

(k) A certification by the Security Officer of the Parties' compliance with the NSA and that there have been no previously unreported Security Incidents or violations of this NSA.

6.4 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 Parties' compliance with the terms of this NSA. In connection with the audit:

(a) Within **60 days** of the CMAs requesting a third-party audit, the Parties will nominate two (2) candidates to serve as third-party auditor that will be subject to CMA approval. The Parties will provide sufficient information for the CMAs to assess the candidates, and the Parties will ensure that each candidate discloses any current or prior contractual, fiduciary, or financial relationship with the Parties. The Parties will ensure that each candidate has the qualifications appropriate to conduct an audit of the Parties' compliance with this NSA.

(b) Within **60 days** of the nominations, the CMAs will approve or disapprove the nominated third-party auditor firms. If the CMAs approve the candidates, the Parties will select one of the two candidates as the third-party auditor.

(c) If the CMAs disapprove of both of the nominated third-party auditors, the Parties agree to nominate another third-party auditor within **30 days** of such disapproval, subject to the approval process as for the initial list of candidates. If the CMAs disapprove the nomination of a supplemental third-party auditor, the Parties will provide to the CMAs two (2) additional candidates within **30 days** to be considered for third-party auditor from whom the CMAs may choose at their discretion.

(d) The Parties will be solely responsible for any costs associated with any third-party audit carried out pursuant to this Section. The CMAs, however, will consider avoidance of unreasonable costs as a factor when exercising their rights under this Section.

---

[3] *See also* Section 2(a) of the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-09); 47 C.F.R. § 1.50000 et seq.

(e) The Parties will ensure the selected third-party auditor submits a draft plan that includes a detailed methodology, approach, scope, and timeline of the audit (the "Audit Plan") to the CMAs within **15 days** following approval of the third-party auditor. If the CMAs disapprove the draft Audit Plan, the Parties, with the third-party auditor, will resolve all concerns raised by the CMAs. If the CMAs approve the Audit Plan, the third-party auditor will begin conducting the Audit.

(f) The Parties will ensure that the executed engagement agreement with the third-party auditor is provided to the CMAs within **5 days** of execution.

(g) The third-party auditor will promptly deliver to the CMAs and the Parties the full Audit Report and related information generated or gathered during its review that relate directly to the Parties' compliance with the terms of this NSA. The third-party auditor will meet independently with the CMAs upon request to discuss any recommendations identified in the Audit Report. The Parties agree to work in good faith with the CMAs regarding how to remediate any concern identified in the Audit Report.

6.5 Consultation and Visitation

(a) The Parties agree to meet and confer with the CMAs and to resolve to the satisfaction of the CMAs any concerns the CMAs may raise regarding compliance with this NSA.

(b) The Parties agree to negotiate in good faith to resolve to the satisfaction of the CMAs any national security or law enforcement concerns the CMAs may raise with respect to any matters set forth in this NSA.

(c) The Parties agree that, upon **48 hours** advance notice, except when due to exigent circumstances such advance notice is not practicable, the CMAs may visit any of the Parties' facilities that are or have been used for discharging the Parties' obligations under this NSA or Quintillion facilities to conduct on-site reviews 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 Parties will cooperate with the requests of the CMAs to make available documents, 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, the Parties will provide the CMAs with access to documents, information, facilities, and personnel within **48 hours** of such an access request.

ARTICLE VII

GENERAL PROVISIONS

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

7.2 Breach. The Parties agree that, in the event that the Parties breach the commitments set forth in this NSA, the Committee may recommend that the FCC modify, condition, revoke, cancel, terminate, enter other declaratory relief, or render null and void any relevant license, permit, or other authorization granted by the FCC to the Parties or any successors-in-interest, in addition to pursuing any other remedy available at law or equity.

7.3 Changed Circumstances. If, after this NSA takes effect, the CMAs or the Parties 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 or law enforcement risks), the Parties and the 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. However, consistent with Executive Order 13913, failure to resolve national security or law enforcement concerns may result in a recommendation that the FCC modify, condition, revoke, cancel, terminate, or render null and void any relevant license, permit, or other authorization granted by the FCC to the Parties or their successors-in-interest, or any other appropriate enforcement action required to address the risks. This NSA may only be modified or terminated by written agreement signed by the Parties and the CMAs.

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

7.5 Forum Selection. A civil action brought by any Signatory to this NSA for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the U.S. District Court for the District of Columbia.

7.6 Compliance with Applicable Law. Nothing in this NSA is intended to excuse the Parties from their obligations to comply with all applicable legal requirements and obligations, including all applicable statutes, regulations, requirements, or orders.

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

(a) For any period stated in days:

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

(ii) every day thereafter is counted (except where business days are specified), including intermediate Saturdays, Sundays, and federal holidays, except for those days that are tolled pursuant to Article 7.7(c); and

(iii) 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.

(b) For any period stated in hours:

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

(ii) count every hour, including hours during intermediate Saturdays, Sundays, and federal holidays, except for those hours that are tolled pursuant to Article 7.7(c); and

(iii) 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.

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

7.8 Other Laws. Nothing in this NSA is intended to limit, alter, or constitute a waiver of:

(a) Any obligation imposed on the Parties by any U.S. federal, state, territory, or local law;

(b) Any enforcement authority available under any U.S. federal, state, territory, or local law;

(c) The sovereign immunity of the United States; or

(d) Any authority or jurisdiction the U.S. government may possess over the activities of the Parties or their agents located within or outside the United States.

7.9 Notification of License Non-Issuance. If, for whatever reason (denial, withdrawal, or other such circumstances), the Parties become aware that the Application is no longer pending before the FCC without having been granted, then the Parties shall notify the CMAs within **24 hours** of the Parties' awareness of such development, including the reason the Application is no longer pending.

7.10 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 Signatory to sign it (the "Effective Date"). If, after this NSA is executed, the Parties fail to receive a license from the FCC (whether due to denial, withdrawal, or other such circumstances), the CMAs and the Parties agree that this NSA automatically terminates.

7.11 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 to have been duly given or made as of the date of receipt and shall be sent by electronic mail addressed to the Signatories' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the Signatories may designate in accordance with this section:

If to the CMAs:

U.S. Department of Homeland Security
Under Secretary for Strategy, Policy and Plans
Office of Strategy, Policy, and Plans
Mail Stop 0445
2707 Martin Luther King Avenue, SE
Washington, D.C. 20528
compliance@hq.dhs.gov

U.S. Department of Justice
Attention: Deputy Chief, Telecommunications &
Deputy Chief, Compliance and Enforcement
National Security Division
Foreign Investment Review Section
175 N Street, NE
Washington, D.C. 20530
Compliance.Telecom@usdoj.gov

U.S. Department of Defense
Office of Foreign Investment Review, Director
Undersecretary of Acquisition and Sustainment
1400 Defense Pentagon
Washington, D.C. 20301
osd.pentagon.ousd-a-s.list.team-telecom@mail.mil

If to Quintillion Subsea Operations, LLC:

Quintillion Subsea Operations, LLC
Attention:
Email:

If to Q Gateway Ultimate Holdings:

Q Gateway Ultimate Holdings
Attention:
Email:
1900 L Street NW, Suite 650, Washington, DC 20006

If to Grain Communications Opportunity Fund III, Master, L.P.:

Grain Communications Opportunity Fund III, Master, L.P.
Attention:
Email:

7.12 Direct Communications. The Parties acknowledge that the CMAs may communicate directly with the Security Officer, Third-Party Auditor and his/her staff, and any other point of contact designated by the Parties. The Parties further acknowledge that the CMAs may respond to communications received directly from any personnel from the Parties regarding the NSA. These acknowledgments shall in no way prohibit or otherwise inhibit the Parties from consulting with, obtaining advice from, or communicating with the CMAs through counsel.

7.13 Notice Regarding Legal Representation. The Parties will identify to the CMAs the contact information for any legal representation as regards compliance with the obligations under this NSA, whether outside legal counsel or internal general counsel, within **5 days** of the NSA's execution, and thereafter shall inform the CMAs within **5 days** of any change to such legal representation.

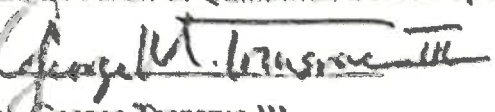
7.14 Severability. The provisions of this Agreement shall be severable and if any provision hereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of such other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

7.15 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.

7.16 Disclosure. The Parties 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.

7.17 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.

For and on behalf of Quintillion Subsea Operations, LLC

By: 

Name: George Tronsrue III

Title: Chief Executive Officer

Contact Information:

Quintillion Subsea Operations, LLC
201 East 56th Avenue, Suite 300
Anchorage, AK 99518
1-800-673-4394
gtronsrue@quintillionglobal.com

Date: December 21, 2023

For and on behalf of Q Gateway Ultimate Holdings

By: Chad A. Crank

Name: Chad Crank

Title: Authorized Signatory; Managing Director of Grain Management, LLC

Contact Information: (202) 779-9051

Date: 12/22/2023

Grain Communications Opportunity Fund III, Master, L.P.

By: Chad A Crank

Name: Chad Crank

Title: Authorized Signatory; Managing Director of Grain Management, LLC

Contact Information: (202) 779-9051

Date: 12/22/2023

For the U.S. Department of Justice

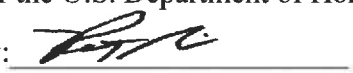
By: _____

Name: Tyler Wood

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

Date: 08 January 2024

For the U.S. Department of Homeland Security

By: 

Name: Robert Silvers

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

Date: 01/02/2024

For the U.S. Department of Defense By: 

Name: Ms. Nicoletta S. Giordani

Title: Director, Global Investment & Economic Security Directorate

Date: January 9, 2024