FILED
10/21/21
04:59 PM

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

In the Matter of the Joint Application of **GTCR Onvoy Holdings, LLC,** *Transferor*, **Onvoy, LLC (U-6487-C),** **Broadvox-CLEC, LLC (U-7160-C),** **ANPI Business, LLC (U-6418-C),** **ANPI, LLC (U-5795-C),** **Neutral Tandem-California, LLC (U-6877-C),** *Licensees*, and **Sinch US Holding Inc.,** *Transferee*, for Approval to Transfer Indirect Control of Licensees to Transferee Pursuant to California Public Utilities Code Section 854(a)	A.21-03-013

SUPPLEMENTAL RESPONSE TO ADMINISTRATIVE LAW JUDGE'S REQUEST FOR ADDITIONAL INFORMATION

GTCR Onvoy Holdings, LLC ("Transferor"); Onvoy, LLC (U-6487-C), Broadvox-CLEC, LLC (U-7160-C), ANPI Business, LLC (U-6418-C), ANPI, LLC (U-5795-C), and Neutral Tandem-California, LLC (U-6877-C) (collectively, the "Licensees"); and Sinch US Holding Inc. ("Transferee") (collectively with Transferor and Licensees, the "Applicants"), submit this Supplemental Response to the following request from the assigned ALJ on September 2, 2021.

2. **Provide all documents filed with the Federal Communications Commission in FCC Docket No. 21-131, including but not limited to: ITC-T/C-20210401-00059; ITC-T/C-20210401-00060; ITC-T/C-20210401-00061; ITC-T/C-20210401-00062; ITC-T/C-20210401-00063; ITC-T/C-20210401-00064; ISP-PDR-20210401-00006**

RESPONSE: Applicants supplement their Response dated September 10, 2021 with **Attachment A**, the Petition to Adopt Conditions to Authorizations and Licenses ("Petition for Conditions") filed by the National Telecommunications and Information Administration ("NTIA")[1] with the Federal Communications Commission ("FCC") dated October 20, 2021, providing that following the review of the Transaction and FCC applications by the Committee for the Assessment of Foreign Participation in the United States Services Sector (the "Committee") the Committee has no objection to the FCC approving the applications provided that the FCC conditions its approval on the assurance that the Applicants abide by the commitments and undertakings set forth in the September 27, 2021 Letter of Agreement ("LOA") attached to the Petition for Conditions. The LOA is a standard method of resolving any national security and law enforcement concerns of the Committee associated with an FCC applicant's foreign ownership. Accordingly, the NTIA letter, included herein as **Attachment A**, evidences that any national security concerns associated with the Transaction have been resolved by the Committee's review and the LOA entered into by the Applicants.

* * * *

Now that NTIA has filed the Petition for Conditions, Applicants currently expect that the FCC will approve the Applications within the next two weeks, *i.e.*, by November 3, 2021. The only other remaining state regulatory approval, from the Mississippi Public Service Commission, is expected November 2, 2021. Applicants have secured approval from, or provided prior notice

[1] The NTIA is part of the Department of Commerce and is the federal Executive Branch agency that is principally responsible for advising the President on telecommunications and policy issues (see https://www.ntia.doc.gov/about).

to, all other states that require such, *i.e.*, 27 states as well as made the requisite filings and obtained the relevant approvals from Puerto Rico and the U.S. Virgin Islands.

Applicants reiterate their request that this Application be considered no later than at the Meeting scheduled for **November 18, 2021**, and if possible at the meeting scheduled for **November 4, 2021**, as Applicants expect that the approvals from the FCC and all other state regulatory agencies will be granted by that date and would like to close the transaction by the end of November. Delay in this Commission's consideration past the Meeting scheduled for November 18, 2021 will impede the parties' ability to integrate and realize the benefits of the Transaction. Moreover, and as detailed in Applicants' response dated September 10, 2021, the Transaction furthers the Commission's goals identified in the Environment and Social Justice Action Plan. Delay in Commission consideration of the Transaction will also delay the public interest benefits this Transaction accomplished.

Additionally, Applicants emphasize that allowing the parties to close the Transaction as quickly as possible furthers important benefits to Applicants' personnel. Specifically, integrating the operations of both companies is a complex endeavor that will take a considerable amount of time to accomplish. Starting this process in advance of the holiday season will provide enormous benefits to personnel and the combined entity alike. A critical part of the integration process is providing personnel with certainty as to what their role will be in the future and allow the combined teams to pursue new opportunities. Delaying these benefits does not benefit any party, including this Commission. Accordingly, Applicants' respectfully request that the Commission consider the Application during the meeting scheduled for **November 4, 2021**, but in no event later than **November 18, 2021**.

Respectfully submitted,

/s/ John T. Nakahata

John T. Nakahata
Henry Shi
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street N.W., 8th Floor
Washington, D.C. 20036-3537
Tel: (202) 730-1348
jnakahata@hwglaw.com
hshi@hwglaw.com

Counsel for Transferee

/s/ Ronald W. Del Sesto, Jr.

Ronald W. Del Sesto, Jr.
Brett P. Ferenchak
Stephany Fan
1111 Pennsylvania Ave., N.W.
Washington, DC 20004-2541
Tel: 202-739-3000
Fax: 202-739-3001
ronald.delsesto@morganlewis.com
brett.ferenchak@morganlewis.com
stephany.fan@morganlewis.com

Counsel for Transferor and Licensees

Dated this 21st day of October, 2021

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

In the Matter of the Joint Application of **GTCR Onvoy Holdings, LLC,** *Transferor*, **Onvoy, LLC (U-6487-C),** **Broadvox-CLEC, LLC (U-7160-C),** **ANPI Business, LLC (U-6418-C)**, **ANPI, LLC (U-5795-C),** **Neutral Tandem-California, LLC (U-6877-C),** *Licensees*, and **Sinch US Holding Inc.,** *Transferee*, for Approval to Transfer Indirect Control of Licensees to Transferee Pursuant to California Public Utilities Code Section 854(a)	A.21-03-013

ATTACHMENT A
TO THE SUPPLEMENTAL RESPONSE TO ADMINISTRATIVE LAW JUDGE'S REQUEST FOR ADDITIONAL INFORMATION

NTIA Petition for Conditions

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Application of	)	
	)	
GTCR Onvoy Holdings, LLC	)	WC Docket No. 21-131
Transferor,	)	ITC-T/C -202 10401-00059
	)	ITC-T/C -202 10401-00060
Sinch US Holding Inc.	)	ITC-T/C -202 10401-00061
Transferee,	)	ITC-T/C -202 10401-00062
	)	ITC-T/C -202 10401-00063
Onvoy, LLC,	)	ITC-T/C -202 10401-00064
Minnesota Independent Equal Access Corporation (MIEAC),	)	ISP-PDR-202 10401-00006
Voyant Communications, LLC,	)	
Broadvox-CLEC, LLC,	)	
ANPIBusiness, LLC	)	
ANPI, LLC,	)	
Inteliquent, Inc., and	)	
Layered Communications, LLC,	)	
Authority Holders,	)	
	)	
For Consent to Transfer Indirect Control of Companies Holding Domestic and International Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended	)	

PETITION TO ADOPT CONDITIONS TO AUTHORIZATIONS AND LICENSES

Pursuant to Executive Order 13913, the National Telecommunications and Information Administration (NTIA) submits this Petition to Adopt Conditions to Authorizations and Licenses (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

[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.

objection to the Commission approving the above-captioned application, provided that the Commission conditions its approval on the assurances of the Authority Holders and Onvoy Spectrum (d/b/a Inteliquent) to abide by the commitments and undertakings set forth in the September 27, 2021, Letter of Agreement (LOA), a copy of which is attached hereto.[2]

Pursuant to section 214(a) of the Communications Act, the Commission must determine whether a proposed transfer of control of any section 214 authorization will serve the public interest, convenience, and necessity.[3] As part of the public interest analysis, the Commission considers whether any such application raises national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's foreign ownership.[4] With regard to these concerns, the Commission has long sought the expertise of the relevant Executive Branch agencies and has accorded deference to their expertise when they have identified such concerns in a particular application.[5]

After discussions with Inteliquent in connection with the above-captioned application, the Committee has concluded that the additional commitments and undertakings set forth in the LOA 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.

---

[2] 47 C.F.R. § 1.41.

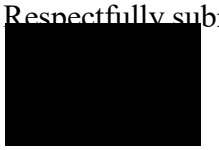
[3] 47 U.S.C. § 214(a); *Applications of Cable & Wireless Plc and Columbus New Cayman Limited for Transfer of Control of Cable Landing Licenses and Section 214 Authorizations*, Memorandum Opinion and Order, 30 FCC Rcd 12730, 12734, ¶ 8 (2015).

[4] *See Market Entry and Regulation of Foreign-affiliated Entities*, Report and Order, 11 FCC Rcd 3873, 3888, ¶¶ 38-39 (1995).

[5] *Id.* at 3888, ¶ 39.

Accordingly, the Committee advises the Commission that it has no objection to the Commission granting the above-captioned application, provided that the Commission conditions its consent on compliance with the September 27, 2021, LOA 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

October 20, 2021

550 West Adams Street
Suite 900
Chicago, IL 60661
+1 312-384-8000
www.inteliquent.com

September 27, 2021

Chief, Foreign Investment Review Section (FIRS)
Deputy Chief, Compliance and Enforcement (FIRS)
On Behalf of the Assistant Attorney General for National Security
United States Department of Justice
National Security Division
175 N Street, NE
Washington, DC 20530

Subject: WC Docket No. 21-131, ITC-T/C-20210401-00059, ITC-T/C-20210401-00060, ITC-T/C-20210401-00061, ITC-T/C-20210401-00062, ITC-T/C-20210401-00063, ITC-T/C-20210401-00064, ISP-PDR-20210401-00006
(TT 21-025 to 032)

Applications by GTCR Onvoy Holdings, LLC (GTCR Holdings), Sinch US Holding Inc. ("Sinch US"), Authority Holders[1] and Onvoy Spectrum, LLC ("Onvoy Spectrum", and collectively with Authority Holders, GTCR Holdings, and Sinch US, "Applicants") for the transfer of control of Authority Holders and Onvoy Spectrum (with Authority Holders collectively d/b/a "Inteliquent") from GTCR Holdings to Sinch US, pursuant to Sections 214 and 310 of the Communications Act of 1934, as amended, and Sections 1.948, 63.03-04, 63.18, and 63.24 of the Federal Communications Commission's rules, requesting consent to transfer control of Authority Holders and Onvoy Spectrum from GTCR Holdings to Sinch US.

Dear Sir/Madam:

This Letter of Agreement ("LOA" or "Agreement") sets forth the commitments that Inteliquent, which includes the Authority Holders and Onvoy Spectrum, makes to the U.S. Department of Justice ("USDOJ"), including the Federal Bureau of Investigation ("FBI"), to address national security and law enforcement risks arising from the Applicants' applications to the Federal Communications Commission ("FCC" or "Commission") requesting consent to transfer control of domestic and international Section 214 authorizations pursuant to Section 214

[1] The Authority Holders consist of Onvoy, LLC ("Onvoy"), Minnesota Independent Equal Access Corporation ("MIEAC"), Voyant Communications, LLC ("Voyant"), Broadvox-CLEC, LLC ("Broadvox"), ANPI, LLC ("ANPI"), ANPI Business, LLC ("ANPI Business"), Inteliquent, Inc. ("Inteliquent"), and Layered Communications, LLC ("Layered").

of the Communications Act of 1934, as amended, 47 U.S.C. § 214, and the implementing regulations at 47 C.F.R. §§ 1.948, 63.03-63.04, 63.18, and 63.24. Sinch US and Onvoy Spectrum also filed a petition for declaratory ruling to permit foreign investment above the 25 percent benchmarks in Section 310(b)(4) of the Act, 47 U.S.C. § 310(b)(4), and Section 1.5000(a)(1), 47 C.F.R. § 1.5000(a)(1), of the Commission's rules.

Inteliquent certifies as true and correct, under penalties outlined in 18 U.S.C. § 1001, all statements it or its representatives have made to USDOJ, the Department of Homeland Security, the Department of Defense, and the FCC in the course of the reviews of the above-referenced applications that were conducted pursuant to Executive Order 13913,[2] and it hereby adopts those statements as the basis for this LOA.

Definitions

1. For purposes of this LOA, the following definitions apply:

a. "Access" means: (1) to enter a location; or (2) to obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise view data or systems in any form, including through information technology (IT) systems, cloud computing platforms, networks, security systems, and equipment (software and hardware). For the avoidance of doubt, Access shall be construed broadly to include rather than exclude considered conduct.

b. "Call Detail Record" ("CDR") means the data records or call log records that contain information about each call made by a user and processed by a switch, call manager, or call server.

c. "Customer Proprietary Network Information" ("CPNI") means as set forth in 47 U.S.C. § 222(h)(1).

d. "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 the organization prompting the need for response and recovery.

e. "Date of FCC Approval" means the date on which the FCC releases a public notice granting the FCC Application.

f. "Domestic Communications" ("DC") means:

(i) Wire Communications or Electronic Communications (whether stored or not), from one location within the United States, including its territories, to another location within the United States; or

[2] 85 Fed. Reg. 19643 (Apr. 8, 2020).

(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.

g. "Domestic Communications Infrastructure" ("DCI") means any Inteliquent system that supports any communications originating or terminating in the United States, including its territories, including 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, Inteliquent to provide, process, direct, control, supervise, or manage DC but would not include the systems of entities for which Inteliquent has a contracted arrangement for interconnection, peering, roaming, long-distance, or wholesale network access.

h. "Electronic Surveillance" means:

(i) The interception of wire, oral, or electronic communications as set forth in 18 U.S.C. § 2510(1), (2), (4) and (12), respectively, and electronic surveillance as set forth in 50 U.S.C. § 1801(f);

(ii) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.;

(iii) Acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as set forth in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.*;*

(iv) Acquisition of location-related information concerning a subscriber or facility;

(v) Preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and

(vi) Access to or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (i) through (v) above and comparable state laws.

i. "Foreign" means non-United States, or its territories.

j. "Geolocation Data" means any information collected by Inteliquent from its customers regarding a customer's location or the customer's device location.

k. "Government" means any government, or governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision, and any court, tribunal, judicial or arbitral body.

l. "Internet Protocol Detail Record" ("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.

m. "Lawful U.S. Process" means U.S. federal, state, or local court orders, subpoenas, warrants, processes, directives, certificates or authorizations, and other orders, legal process, statutory authorizations and certifications for Electronic Surveillance, physical search and seizure, production of tangible things or Access to or disclosure of DC, call-associated data, transactional data, Subscriber Information, or associated records.

n. "Managed Network Service Provider" ("MNSP") means any third party that has Access to Principal Equipment for the purpose of:

(i) network operation; provisioning of Internet and telecommunications services; routine, corrective, and preventative maintenance, including switching, routing, and testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, creation and implementation of modifications or upgrades; or

(ii) provision of DC or operation of DCI, including: customer support; Operations Support Systems ("OSS"); Business Support Systems ("BSS"); Network Operations Centers ("NOCs"); information technology; cloud operations/services; 5G (Software Defined Networking, Network Function Virtualization, Applications); and datacenter services and operations.

o. "Network Operations Center" ("NOC") means any locations and facilities performing network management, monitoring, accumulating accounting and usage data, maintenance, user support, or other operational functions for DC.

p. "Offshore" means performing obligations of this LOA using entities and personnel outside of the territorial limits of the United States, whether or not those entities or personnel are employees of Inteliquent.

q. "Outsource" means, with respect to DC, supporting the services and operational needs of Inteliquent at issue in this LOA using contractors or third parties.

r. "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 his or her 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.

s. "Principal Equipment" means all telecommunications and information network equipment (*e.g.*, hardware, software, platforms, OS, applications, protocols) that supports core telecommunications or information services, functions, or operations.

t. "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.

u. "Security Incident" means:

(i) Any known or suspected breach of this LOA, including a violation of any approved plan, policy, or procedure under this LOA;

(ii) Any unauthorized Access to, or disclosure of U.S. Records;

(iii) Any unauthorized Access to, or disclosure of, information obtained from or relating to Government entities; or

(iv) Any one or more of the following which affect the company's computer network(s) or associated information systems:

A. Unauthorized disruptions to a service or denial of a service;

B. Unauthorized processing or storage of data;

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

D. Unplanned incidents that cause activation of Inteliquent's Cybersecurity Incident Response Plan;

E. Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect the company's ability to comply with the terms of this LOA; or

F. 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.

v. "Sensitive Personal Data" means sensitive personal data as set forth in 31 C.F.R. § 800.241.

w. "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.

x. "U.S. Records" means Inteliquent's customer billing records, Subscriber Information, PII, Sensitive Personal Data, CDRs, IPDRs, CPNI, Geolocation Data, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by Inteliquent 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.

Law Enforcement Point of Contact

2. Inteliquent agrees to designate and maintain a U.S. law enforcement point of contact ("LEPOC") in the United States who will be subject to prior approval by USDOJ, including the FBI. The LEPOC shall be a U.S. citizen residing in the United States or its territories unless USDOJ otherwise agrees in writing. The LEPOC must be approved by the FBI to receive service of Lawful U.S. Process for U.S. Records and, where possible, to assist and support lawful requests for surveillance or production of U.S. Records by U.S. federal, state, and local law enforcement agencies.

3. Inteliquent agrees to provide the LEPOC's PII to USDOJ within 15 days of the Date of FCC Approval. USDOJ agrees to object or non-object within 15 days from receiving the LEPOC's PII.

4. Inteliquent agrees to notify USDOJ, including the FBI, in writing at least 30 days prior to modifying its LEPOC for USDOJ and FBI objection or non-objection. For those cases involving the unexpected firing, resignation, or death of the LEPOC, written notice will be provided within five days of such event. Under these circumstances, USDOJ and FBI will object or non-object to the replacement LEPOC within 30 days of notification.

5. Inteliquent agrees that the designated LEPOC will have Access to all U.S. Records, and, in response to Lawful U.S. Process, will make such records available promptly and, in any event, will respond to the request no later than five days after receiving such Lawful U.S. Process unless USDOJ grants an extension.

Personnel Screening

6. Inteliquent agrees to implement, either directly or through a vendor, a process to screen existing or newly hired Inteliquent personnel or any personnel of an approved Outsourced or Offshored service provider performing under an agreement with Inteliquent. The personnel screening process shall include background investigations, public criminal records checks, or other analogous means to ascertain a person's trustworthiness. Inteliquent further agrees to provide USDOJ with a written description of this personnel-screening process no later than 60 days after the Date of FCC Approval for USDOJ objection or non-objection. USDOJ agrees to object or non-object within 60 days of receiving notice.

7. Inteliquent agrees to notify USDOJ of all its Foreign person employees, or Foreign person employees of approved Outsourced or Offshored service providers, that it intends to allow Access to U.S. Records, DC, or DCI. Inteliquent agrees to make such notification no less than 30 days prior to the date by which it is seeking such Access be granted; or, with respect to any Foreign persons with such Access as of the Date of FCC Approval, within 30 days of the Date of FCC Approval for USDOJ objection or non-objection. Inteliquent further agrees to provide the PII to USDOJ for each Foreign person so identified. USDOJ agrees to object or non-object within 30 days of receiving notice.

Security Officer

8. Inteliquent agrees to designate and maintain a security officer ("Security Officer") who is a non-dual United States citizen residing in the United States, and may also designate and maintain an alternate security officer ("Alternate Security Officer") to fulfill the responsibilities of the Security Officer in the event of his or her unavailability. The Security Officer and any Alternate Security Officer will be eligible, at the sole discretion of the USDOJ, to hold and maintain a U.S. Government security clearance at the "Secret" level or higher immediately upon appointment. The Security Officer and any Alternate Security Officer will have the appropriate authority and skills to implement the terms of this LOA and to address security concerns identified by the USDOJ. The Security Officer and any Alternate Security Officer will have the appropriate senior-level corporate authority within Inteliquent to perform his or her duties under this LOA. The Security Officer and any Alternate Security Officer will possess the necessary resources and skills to enforce this LOA and to act as a liaison to the USDOJ regarding compliance with this LOA and to address any national security or law enforcement issues arising during Inteliquent's due course of business. Inteliquent will provide the Security Officer and any Alternate Security Officer with Access to Inteliquent's business information that is necessary for the Security Officer and any Alternate Security Officer to perform his or her duties.

9. The Security Officer will be available 24 hours per day, 7 days per week, to respond to and address any national security or law enforcement concerns that USDOJ may raise with respect to Inteliquent or its operations, except if Inteliquent designates an Alternate Security Officer, then in the event that the Security Officer is unavailable, the Alternate Security Officer will be available to respond to and address such concerns. Upon request by USDOJ, the Security Officer or, as applicable, Alternate Security Officer, will make himself or herself available in person within the United States or its territories within 72 hours, at a date and location, including in a classified setting, as deemed necessary by USDOJ.

10. Inteliquent agrees to nominate a proposed candidate for Security Officer to USDOJ within 15 days from the Date of FCC Approval, and thereafter will provide at least 10 days' notice of a Security Officer's departure, and 30 days' prior notice of a new Security Officer designation (except in the case of the unexpected firing, resignation, or death of the Security Officer in which case such written notice of such departure or designation must be provided within five days of such event) of such proposed change. Inteliquent further agrees not to maintain a vacancy or suspension of the Security Officer position for a period of more than 60 days. In the event that Inteliquent designates an Alternate Security Officer, Inteliquent will nominate a proposed candidate for Alternate Security Officer at least 30 days prior to the date on which Inteliquent proposes to designate an Alternate Security Officer. All Security Officer

nominations and any Alternate Security Officer nominations will be subject to USDOJ review and objection or non-objection within 30 days from receipt of the nomination and may be subject to a background check at the sole discretion of USDOJ. Inteliquent agrees to address concerns raised by USDOJ regarding the selection and identity of the Security Officer and any Alternate Security Officer.

Lawful U.S. Process and Requests for Information

11. Inteliquent agrees to comply with all applicable lawful interception statutes, regulations, and requirements, as well as comply with all court orders and other Lawful U.S. Process for lawfully authorized Electronic Surveillance. Inteliquent further agrees to certify to USDOJ its compliance with the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001-1010, and its implementing regulations, within 30 days from the Date of FCC Approval.

12. Inteliquent agrees to provide notice of any material modification to its lawful intercept capabilities to USDOJ within 30 days of such modification, and will re-certify its compliance with CALEA no more than 60 days following its notice to USDOJ of any material new facilities, services, or capabilities.

13. Upon receipt of any Lawful U.S. Process, Inteliquent agrees to place any and all information responsive to the Lawful U.S. Process within the territorial boundaries of the United States and otherwise provide information to the requesting officials, in a manner and time consistent with the Lawful U.S. Process.

14. Inteliquent agrees not to provide, or otherwise allow the disclosure of, or Access to, U.S. Records, DCI, DC, or any call content or call data information, to any Foreign Government, or any Foreign person not approved pursuant to Paragraph 7 of this LOA, without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

15. Inteliquent agrees not to disclose the receipt of Lawful U.S. Process, or compliance with Lawful U.S. Process, to any Foreign Government, or any person not authorized under the Lawful U.S. Process, without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

16. Inteliquent agrees to refer any requests for information or Access described in Paragraph 14 from a Foreign person not approved pursuant to Paragraph 7 or a Foreign Government, including any legal process from a Foreign Government, to USDOJ as soon as possible, but in no event later than five days after such a request, or legal process, is received by, or made known to, Inteliquent, unless disclosure of the request, or legal process, would be in violation of U.S. law, or in violation of an order of a court of competent jurisdiction in the United States.

17. Inteliquent agrees not to comply with such requests from Foreign Governments and Foreign persons without prior written consent of USDOJ, or an order of a court of competent jurisdiction in the United States.

18. Inteliquent agrees to ensure that U.S. Records are not subject to mandatory destruction under any Foreign laws.

Unauthorized Access and Security Incidents

19. Inteliquent agrees to take all practicable measures to prevent unauthorized Access to U.S. Records, DC, and the DCI.

20. Inteliquent agrees to take all practicable measures to prevent any unlawful use or disclosure of information relating to U.S. Records or DC.

21. Inteliquent agrees to prepare: (1) a Cybersecurity Plan; and (2) a comprehensive System Security Plan ("SSP") (together the "Plans"), each of which shall be guided by the current version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and incorporate applicable controls found in NIST SP 800-53, NIST SP 800-171, or other international information security standards. Inteliquent will provide copies of those Plans to USDOJ within 60 days of the Date of FCC Approval for objection or non-objection. Furthermore, Inteliquent agrees that the Plans will be updated when appropriate to conform with evolving information security standards, and Inteliquent will make additional modifications to these Plans, if requested by USDOJ, and to work with USDOJ to implement such modifications. USDOJ agrees to object or non-object within 60 days of receiving each version of the Plans.

22. Inteliquent agrees that its Plans will include, among other things, policies relating to its information security, supply chain security, cybersecurity incident response, remote access, physical security, cybersecurity, third-party contractors, Outsourcing and Offshoring, maintenance and retention of system logs, protection of Lawful U.S. Process, protection of U.S. Records obtained by Inteliquent in the ordinary course of business, and Inteliquent's plans regarding new contracts or amendments to existing contracts with third-party providers requiring those third parties to notify Inteliquent in the event of a breach or loss of U.S. Records within a specified time period after discovery, not to exceed 72 hours from the time of discovery.

23. Inteliquent agrees to provide to USDOJ updated network diagrams and topology maps showing all facilities, devices, interfaces, PoPs, exchange points, and NOCs within 60 days from the Date of FCC Approval.

24. Inteliquent agrees to notify USDOJ at least 30 days prior to changing the location for storage of U.S. Records. Such notice shall include:

a. A description of the type of information to be stored in the new location;
b. The custodian of the information (even if such custodian is Inteliquent);
c. The location where the information is to be stored;
d. Updated SSP and Cybersecurity Plans detailing the physical/logical protections at the new location; and
e. The factors considered in deciding to store that information in the new location.

USDOJ agrees to object or non-object to the location within 60 days of receiving notice.

Reporting Incidents and Breaches

25. Inteliquent agrees to report in writing to USDOJ promptly, and in any event no later than 48 hours, after if it learns of information that reasonably indicates a known or suspected:

a. Security Incident;
b. Unauthorized Access to, or disclosure of, any information relating to services provided by Inteliquent, or referring or relating in any way to Inteliquent's customers in the United States or its territories;
c. Any unauthorized Access to, or disclosure of, DC in violation of federal, state, or local law; or
d. Any material breach of the commitments made in this LOA.

26. Inteliquent agrees to require any third-party service provider to disclose to Inteliquent any data breach of any U.S. Records, or any loss of U.S. Records, whether from a data breach, or other cause, within 72 hours of the third party discovering the breach or loss. Inteliquent agrees further to require any third-party service provider to disclose to Inteliquent, within 72 hours of discovery, any critical exposure, threat, and vulnerabilities activating its Cybersecurity Incident Response Plan, associated with the products or services provided to Inteliquent, 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.

27. Inteliquent further agrees to take timely and appropriate remedial measures, as recommended by the US-Computer Emergency Readiness Team/Cybersecurity and Infrastructure Security Agency ("US-CERT"/"CISA"), an Information Sharing and Analysis Center ("ISAC"), or other authority, to respond and recover from any cyber or supply chain incident and mitigate vulnerabilities.

28. Inteliquent agrees to notify USDOJ, including the points of contact ("POCs") listed in this LOA, in writing of any of the Security Incidents or breaches described in this LOA. Such notification shall take place no later than 48 hours after Inteliquent has knowledge of, or is informed by a third party providing Outsourced or Offshored services to Inteliquent of, the incident, intrusion, or breach has taken or is taking place, or sooner when required by statute or regulations.

29. Inteliquent agrees to notify the FBI and U.S. Secret Service as provided in 47 C.F.R. § 64.2011 within seven business days after reasonable determination that a person without authorization, or in exceeding their authorization, has gained Access to, used, or disclosed CPNI, whether through Inteliquent's network or that of a third party used by Inteliquent, and shall electronically report the matter to the central reporting facility through the following portal: https://www.cpnireporting.gov

Principal Equipment

30. Inteliquent agrees to provide USDOJ, within 30 days of the Date of FCC Approval, a Principal Equipment list. The Principal Equipment list shall include the following:

a. A complete and current list of all Principal Equipment, including:

(i) a description of each item and the functions supported,
(ii) each item's manufacturer, and
(iii) the model and/or version number of any hardware or software.

b. The name, address, phone number, and website for any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment.

USDOJ agrees to object or non-object to the Principal Equipment List within 60 days of its receipt.

31. Inteliquent agrees to notify USDOJ in writing at least 30 days prior to introducing any new Principal Equipment or modifying any of its Principal Equipment. USDOJ agrees to object or non-object to such new Principal Equipment or modification to the Principal Equipment within 30 days of receiving notice.

32. Inteliquent agrees to provide USDOJ with the name, address, phone number, and website of any providers, suppliers, and entities that will perform any maintenance, repair, or replacement that may result in any introduction of new Principal Equipment or modification to its Principal Equipment or systems or software used with or supporting the Principal Equipment. USDOJ agrees to object or non-object to the nominated providers, suppliers, and entities selected by Inteliquent within 30 days of receiving notice.

Outsourced and Offshored Services

33. Inteliquent agrees to provide the USDOJ within 30 days of the Date of FCC Approval, a list of all Outsourced or Offshored service providers that provide services to Inteliquent for USDOJ objection or non-objection. The list should include any Outsourced or Offshored service provider that provides services for:

a. MNSP services;
b. NOC(s);
c. Network maintenance services;
d. Billing or customer support services;
e. Any operation or service that could potentially expose the DCI, DC, or U.S. Records; and
f. Deploying any network elements, hardware, software, core network equipment, and network management capabilities that are owned, managed, manufactured, or controlled by a Foreign Government or non-public entities.

Inteliquent further agrees to provide the name, address, phone number, website, and description of services provided for each Outsourced or Offshored provider included on the list submitted to USDOJ pursuant to this paragraph. USDOJ agrees to object or non-object to the Outsourced and Offshored service provider list within 60 days of receiving notice.

34. Inteliquent agrees to notify USDOJ in writing no less than 30 days prior to the use of any new Outsourced or Offshored service providers that will provide any of the services described in Paragraph 33. Inteliquent agrees that such notification shall include all of the identifying information contained in Paragraph 33 for the new Outsourced and Offshored service provider.

35. USDOJ agrees to object or non-object to any new Outsourced or Offshored service providers within 30 days of receiving notice.

Network Operations Centers

36. Inteliquent agrees to notify USDOJ in writing at least 60 days prior to changing the location of its NOCs. Inteliquent will provide the address, owner (even if Inteliquent), Principal Equipment, and MNSP (as well as any new Outsourced or Offshored service providers) of the NOC with the notification, as well as appropriately updated SSP and Cybersecurity Plans. USDOJ agrees to object or non-object to the proposed NOC location within 60 days of receiving notice.

Change in Ownership and Service Portfolio

37. Inteliquent agrees to provide USDOJ notice of any changes to its business, including but not limited to corporate structure changes, ownership changes other than Sinch AB non-controlling ownership changes and *pro forma* transactions as defined in 47 C.F.R. § 63.24(f), corporate name changes, business model changes, corporate headquarter location changes, or business operation location changes no less than 30 days in advance of such change. Inteliquent also agrees to provide USDOJ notice within 30 days of initiating any bankruptcy proceeding or any other legal proceeding undertaken for the purpose of liquidating, reorganizing, refinancing, or otherwise seeking relief from all or some of Inteliquent's debts. With respect to Sinch AB non-controlling ownership changes, Inteliquent agrees to provide USDOJ with notice within 15 days of the date Sinch AB becomes aware of the acquisition of a five-percent-or-greater interest by any investor not previously disclosed to USDOJ. With respect to *pro forma* changes in ownership or corporate structure, Inteliquent agrees to provide USDOJ with notice concurrently with the notice required to be filed with the FCC.

38. Inteliquent agrees to provide USDOJ notice of any material change to its current portfolio of services offering, including offering other services beyond its current service portfolio, no less than 30 days in advance of such change. USDOJ will object or non-object to the proposed new services within 30 days of receiving notice.

Annual Report

39. Inteliquent agrees to provide an annual report to USDOJ regarding the company's compliance with this LOA, to include:

a. Certification that there were no changes during the preceding year (where no changes were reported to USDOJ during the year);

b. Notice(s) regarding the company's handling of U.S. Records, DC, and Lawful U.S. Process (*i.e.,* whether handled properly and in accordance with the assurances contained herein) including a list of individuals with access to U.S. Records, DC, and DCI;
c. Notification(s) of the installation and/or purchase or lease of any Foreign-manufactured Principal Equipment;
d. Notification(s) of any relationships with Foreign-owned telecommunications partners, including any network peering (traffic exchange) or interconnection relationships;
e. Updated network diagrams and topology maps showing all facilities, devices, interfaces, PoPs, exchange points, and NOCs;
f. Updated SSP and Cybersecurity Plan;
g. Updated organizational chart showing all owners with a 5% or greater ownership share;
h. Report(s) of any occurrences of Security Incidents;
i. A re-identification of the location that Inteliquent stores U.S. Records and the types of U.S. records collected and stored;
j. A re-identification of the name of and contact information of the LEPOC and Security Officer;
k. Notification of all filings or notices to the FCC in the prior year, and a copy of these filings if requested by USDOJ;
l. Certification of compliance with CALEA and any other applicable U.S. lawful interception statutes, regulations, and requirements;
m. A description of the services that Inteliquent provides in the United States and the specific services provided using the domestic and international Section 214 authorizations as well as services it provides in the United States that do not require Section 214 authority (to include a description of any services provided to government or critical infrastructure customers); and
n. Notification of any reasonably foreseeable matter that would give rise to an obligation under this LOA.

The annual report will be due one year after the Date of FCC Approval and every year thereafter. Inteliquent agrees to send electronic copies of the annual report and all notices and communications required under this LOA to the following individuals or any other individuals that DOJ identifies to Inteliquent in the future: Eileen Keenan, USDOJ (at Eileen.Keenan@usdoj.gov); Loyaan Egal, USDOJ and Eric Johnson, USDOJ (at Compliance.Telecom@usdoj.gov). Upon USDOJ request, Inteliquent agrees to provide USDOJ with paper copies of any annual report, notices, or communications required under this LOA.

Site Visits

40. Inteliquent agrees to permit USDOJ's requests for site visits and information, approve all requests to conduct on-site interviews of Inteliquent employees, and provide all documents necessary to verify the implementation of and compliance with the terms of this LOA, or to identify grounds for modification of this LOA.

Miscellaneous

41. Inteliquent agrees 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.

42. If USDOJ finds that the terms of this LOA are inadequate to resolve any national security or law enforcement concerns, Inteliquent agrees to resolve USDOJ's concerns, according deference to the USDOJ's views on the need for modification. Rejection of a proposed modification shall not alone be dispositive, but failure to resolve national security or law enforcement concerns may result in a request 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 Inteliquent or its successors-in-interest, or any other appropriate enforcement action required to address the concern.

43. Inteliquent agrees that in the event that Inteliquent breaches the commitments set forth in this LOA, to include conduct contrary to timely USDOJ objection to any notice submitted pursuant to this LOA, a recommendation may be made that the FCC modify, condition, revoke, cancel, enter other declaratory relief, or render null and void any relevant license, permit, or other authorization granted by the FCC to Inteliquent or its successors-in-interest, in addition to pursuing any other remedy available by law or equity.

44. For purposes of counting days in this LOA, the day of the event that triggers the period is excluded, but every day thereafter is counted, including intermediate Saturdays, Sundays, and legal holidays. Include the last day of the period, but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or legal holiday.

45. Inteliquent agrees that this agreement supersedes the November 21, 2017 LOA between Onvoy Spectrum, LLC and USDOJ.

46. Inteliquent understands that, upon execution of this LOA by an authorized representative or attorney, or shortly thereafter, the FCC will be notified that there is no objection to grant of the application.

Sincerely,

Richard L. Monto
September 27, 2021
Inteliquent