[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of ARCOS-1 USA, INC. A.SURNET, INC. Application for a Modification to Cable Landing License	File No. SCL-MOD-20210928-00039

Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application

TABLE OF CONTENTS

I. Introduction

For the following reasons as well as those in the accompanying classified annex,[1] the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Committee")[2] recommends that the Federal Communications Commission ("FCC") deny this cable-landing license application to modify the ARCOS-1 Cable System to include a new authorized landing point in Cojimar, Cuba.

The United States supports the Cuban people's access to an open, interoperable, secure, and reliable internet, and the Department of State's 2019 Cuba Internet Task Force Final Report recommends support for the construction of a new submarine cable. However, the application to land this subsea cable in Cuban territory, as proposed, should be denied. This proposal presents immitigable risks to the national security and law enforcement interests of the United States.

These risks are posed by the current Cuban government, not the Cuban people. As the President has reiterated, the "United States stands with the Cuban people."[3] Ensuring that "the Cuban people have safe and secure access to the free flow of information" on the internet is important in supporting their democratic self-determination, and the United States has condemned the Cuban government's repression, internet disruptions, network restrictions, and other censorship measures that block the Cuban people's safe and secure access to internet and telecommunications services.[4]

Subsea cables are the backbone of global communications critical infrastructure. Because they carry most of the world's internet, voice, and data traffic between continents, subsea cables have become an increasingly data-rich environment vulnerable to exploitation by foreign adversaries, as the Committee has previously explained and the FCC has recognized. This application requests a license to create the only direct, currently operable commercial cable connection between the United States and Cuba.

Cuba's state-owned telecommunications monopoly, Empresa de

---

[1] Although this unclassified recommendation independently supports the Committee's denial recommendation without the need to rely on the classified annex, the classified annex provides supplemental information that lends additional support to the recommendation.

[2] This filing is made in coordination with Committee Advisors in accordance with subsections 3(d) and 9(f) of Executive Order 13913. *See Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, 85 Fed. Reg. 19643 (Apr. 8, 2020).

[3] The White House, *Fact Sheet: Biden-Harris Administration Measures on Cuba* (July 22, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/22/fact-sheet-biden-harris-administration-measures-on-cuba/; *see, e.g.*, The White House, National Security Strategy 41 (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; Proclamation 10423, 87 Fed. Reg. 43199 (July 15, 2022).

[4] Fact Sheet: Biden-Harris Administration Measures on Cuba, *supra* note 3.

Telecomunicaciones de Cuba S.A. ("ETECSA"), would own the cable-landing station ("CLS") in Cuba, [redacted], and control the operation of the newly proposed segment ("Segment 26") of the cable from the Cuban side. Through ETECSA, the Government of Cuba—which the United States recognizes as authoritarian and a foreign adversary[5]— could access and collect all U.S. persons' internet traffic, sensitive data, and communications transiting Segment 26. This risk of access is not limited to U.S. traffic destined for Cuba. There are several ways in which traffic destined for places outside Cuba, which otherwise would not traverse Cuban networks, could nonetheless be misrouted by ETECSA or otherwise re-routed over this cable into Cuban territory and into the Cuban government's hands. The Cuban government's access to this cable can thus advance its intelligence-collection objectives by giving it direct access to the U.S. persons' communications and sensitive data traversing the cable.

These risks are exacerbated by the Cuban government's relationships with other foreign adversaries, including the People's Republic of China and the Russian Federation. The Cuban government may share any information collected from this cable with those foreign adversaries—thereby advancing counterintelligence efforts against the United States.

Given the current political landscape on the island, the proposed cable landing may not advance the important objective of expanding the free flow of information to the Cuban people and supporting their democratic self-determination at this time. Additionally, given the Cuban government's ownership, use, and control of the cable through ETECSA (an entity directly owned by a foreign adversary that, at present, could not be a trusted party to an agreement with the Committee to potentially mitigate the specific risks of the cable modification proposed by this application), the significant counterintelligence threat posed by the Cuban government itself, and its close relationships with other foreign adversaries, this application presents national security and law enforcement risks that cannot be mitigated. The FCC should deny the application.

II. Legal Authority

A. The FCC's Authority Over Cable-Landing Licenses

The Cable Landing License Act of 1921 ("CLLA") authorizes the President to grant, withhold, revoke, or impose conditions on cable-landing licenses,[6] and the President delegated that authority to the FCC in Executive Order ("E.O.") 10530.[7] That E.O., as well as the FCC's own regulations, require the FCC to obtain approval

---

[5] *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. at 4911 (January 19, 2021).

[6] 47 U.S.C. §§ 34–39.

[7] E.O. 10530 § 5(a), 19 Fed. Reg. 2709 (May 10, 1954); *see also Rules and Policies on Foreign Participation in the U.S. Telecommunications Mkt.*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23922, ¶ 87 (1997) [hereinafter *1997 Foreign Participation Order*].

from the Secretary of State and to seek advice from other Executive Branch departments and agencies as necessary (including the Committee) before granting or revoking any such license.[8]

The CLLA gives the President (and the FCC by delegation) broad authority to regulate cable-landing licenses, including granting them conditioned on appropriate mitigation measures.[9] Under section 2 of the CLLA, the President has discretion to withhold, revoke, or impose conditions on cable-landing licenses if the President determines "after due notice and hearing that such action[s] will assist in securing rights for the landing or operation of cables in foreign countries, or in maintaining the rights or interests of the United States or of its citizens in foreign countries, or will promote the security of the United States[.]"[10]

This authority is broad, as FCC regulations elaborate. For example, the FCC has expressly declined to limit its review of cable-landing license applications to the U.S. landing party and landing station, instead reviewing all entities with a five percent or greater ownership interest in a cable system and using the U.S. points of the cable system to receive a license before landing or operating a cable.[11] As the FCC has explained, because cable management decisions are often made through committees or consortia of owners, a foreign or domestic firm's influence on cable operations "falls squarely within the ambit of the Cable Landing License Act, which requires a license to 'land or operate' a submarine cable."[12]

B. The Committee's Role

Under E.O. 13913, the Department of Justice ("DOJ"), the Department of

---

[8] E.O. 10530 § 5(a); *see also 1997 Foreign Participation Order*, 12 FCC Rcd at 23922, ¶ 87; 47 C.F.R. § 1.767(b) (2019) (authorizing the FCC to act upon a cable-landing license application only "after obtaining the approval of the Secretary of State and such assistance from any executive department or establishment of the Government as it may require").

[9] *See generally* 47 U.S.C. § 35; 47 C.F.R. § 1.767(g)(10); E.O. 13913 §§ 3(a)(ii), 4(a)(iv), 9(a)(iii), 10(a); *see, e.g.*, *Citgo Petroleum Corp. v. U.S. Foreign Trade Zones Bd.*, 83 F.3d 397, 400 (Fed. Cir. 1996); *Shanty Town Assocs. Ltd. P'ship v. EPA*, 843 F.2d 782, 789 n.11 (4th Cir. 1988).

[10] *Id.*; *see also 1997 Foreign Participation Order*, 12 FCC Rcd at 23946 n.252 (stating that 47 U.S.C. § 35 "gives [the FCC] discretion to deny an application if to do so would . . . promote the security of the United States"); *Telefonica Larga Distancia de Puerto Rico, Inc.*, Memorandum Opinion and Order, 12 FCC Rcd 5173, 5181–82, ¶¶ 23–25 (1997) [hereinafter *Telefonica Puerto Rico*] (denying a cable-landing license application after the State Department, in coordination with DoD, NTIA, and USTR, sent a letter to the FCC stating that the license application should be denied, on the basis that denial would assist in maintaining the rights of U.S. corporations in a foreign country).

[11] 47 C.F.R. § 1.767(h)(2); *see also Review of Commission Consideration of Applications under the Cable Landing License Act*, Report and Order, 16 FCC Rcd 22167, 22196–97, ¶ 57 (2001) [hereinafter *2001 Cable Landing Order*] (declining to limit applicants to landing parties); *Review of Commission Consideration of Applications under the Cable Landing License Act*, Notice of Proposed Rulemaking, 15 FCC Rcd 20789, 20824, ¶ 82 (2000) ("We note that the greater a firm's investment in a cable system, the greater ability the firm has to influence the way in which a cable is operated.").

[12] *2001 Cable Landing Order*, 16 FCC Rcd at 22197, ¶ 57 (emphasis in the original).

Homeland Security ("DHS"), and the Department of Defense ("DOD") comprise the Members of the Committee, whose primary objective is to assist the FCC in its public-interest review of national security and law enforcement concerns that may be raised by foreign participation in the U.S. telecommunications services sector.[13] The Committee reviews applications referred by the FCC for risks to U.S. national security and law enforcement interests. Based on its review, the Committee advises the FCC on the disposition of the application—non-objection to granting the application, a recommendation that the FCC only grant the license contingent on the applicant's compliance with mitigation measures to address the risks identified, or a recommendation that the FCC deny the application due to the risk to the national security or law enforcement interests of the United States where such risks cannot be mitigated.[14]

The FCC has long treated national security and law enforcement concerns as important public interest factors in the advice that the FCC seeks from other Executive Branch agencies.[15] The FCC will "accord deference to the expertise of Executive Branch agencies in identifying and interpreting issues of concern related to national security, law enforcement, and foreign policy[.]"[16] This advice "must occur only after appropriate coordination among Executive Branch agencies, must be communicated in writing, and will be part of the public file in the relevant

---

[13] E.O. 13913 § 3(a), 85 Fed. Reg. 19643 (Apr. 8, 2020).

[14] *Id.* § 9(a); *1997 Foreign Participation Order*, 12 FCC Rcd at 23946, ¶ 130 (noting that the FCC will "continue to consider, . . . other factors consistent with our discretion under the Submarine Cable Landing License Act that may weigh in favor of or against grant of a license"); *see also id.* n.252 (noting that the FCC's analysis under Section 2 of that Act includes "discretion to deny an application if to do so would . . . 'promote the security of the United States'"); *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, FCC 20-133, Report and Order, 35 FCC Rcd 10927 (Oct. 1, 2020) [hereinafter *Executive Branch Review Order*] (adopting rules and procedures to streamline and improve the efficiency and transparency of the process by which the FCC coordinates with Executive Branch agencies for assessment of any national security, law enforcement, foreign policy, and/or trade policy issues related to certain applications filed with the FCC).

[15] *1997 Foreign Participation Order*, 12 FCC Rcd at 23919–20, ¶¶ 62–63; *see also Executive Branch Review Order*, 35 FCC Rcd at 10928–31, ¶¶ 3–7.

[16] *Foreign Participation Order*, 12 FCC Rcd at 23920, ¶ 63; ***s**ee also* Reform of Rules and Policies on Foreign Carrier Entry into the U.S. Telecommunications Market, Report and Order, 29 FCC Rcd 4256, 4258, ¶ 4 (2014) [hereinafter 2014 Foreign Carrier Entry Order] ("The [FCC]'s presumption, however, is limited to competition issues; it does not apply to questions regarding national security, law enforcement, foreign policy or trade policy concerns, and such questions are resolved in the same manner regardless of the WTO status of the carrier's home country. The [FCC] accords deference to Executive Branch agencies in identifying and interpreting issues of concern related to these matters."); *Telefonica Puerto Rico*, 12 FCC Rcd at 5182–85 ¶¶ 24–33 (adopting the State Department's disapproval of a proposed cable application, in coordination with the advice of DoD, NTIA, and USTR, and noting State Department's determination that "grant of the applications would be inconsistent with the rights and interests of U.S. companies that desire to compete in the Spanish telecommunications market").

proceeding."[17]

E.O. 13913 established formal processes for the Committee to follow in reviewing applications (including for submarine cable-landing licenses) for national security and law enforcement concerns.[18] If the Committee decides to recommend that the FCC deny an application, the Committee must first notify the Committee Advisors and consult them on their views as to the recommendation.[19] The Committee Advisors have 21 days to advise the Chair whether they oppose the recommendation; if a Committee Advisor does so, then the Committee and the Advisors follow the process established under E.O. 13913 to try resolve any opposition and reach consensus.[20] If there is no opposition, the Committee provides its recommendation to the FCC.

III. The Application to Modify the ARCOS-1 Cable System

A. Applicants

Applicants ARCOS-1 USA, Inc. and A.SurNet, Inc.—both Delaware corporations with their principal place of business in Miami, Florida[21]—have applied to modify their existing cable-landing license for the ARCOS-1 Cable System.

A consortium owns the existing ARCOS-1 Cable System. Applicants' intermediate parent, Columbus Networks, Limited ("CNL")—an international telecommunications services company incorporated and headquartered in Barbados—[redacted]

[17] *1997 Foreign Participation Order*, 12 FCC Rcd at 23921, ¶ 66; *see also id.* at n.121 ("To the extent the Executive Branch must share classified information with [FCC] staff, such information is not subject to public disclosure.").

[18] *See generally* E.O. 13913, 85 Fed. Reg. 19643 (Apr. 8, 2020).

[19] *Id.* § 9(f). The Committee Advisors consist of the Secretary of State, Secretary of the Treasury, Secretary of Commerce, Director of the Office of Management & Budget, United States Trade Representative, Director of National Intelligence, Administrator of General Services, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, Director of the Office of Science and Technology Policy, and the Chair of the Council of Economic Advisors (plus any other Assistants to the President that the President designates). *Id.* § 3(d).

[20] *See id.* § 9(f).

[21] The Applicants are indirectly wholly owned by CNL, an international telecommunications services company incorporated and headquartered in Barbados. CNL is a wholly owned, indirect subsidiary of Cable & Wireless Communications Limited, an international telecommunications company incorporated and headquartered in England. Liberty Latin America Ltd. ultimately wholly owns the Applicants and their intermediate parent companies. Liberty Latin America Ltd. is an international provider of cable and telecommunications services incorporated and headquartered in Bermuda. A U.S. citizen (John C. Malone) holds a 15% equity interest and 31% voting interest in Liberty Latin America Ltd. No other individuals or entities hold a 10% or greater voting or equity interest in ARCOS-1 USA, Inc. or A.SurNet, Inc. as a result of their voting or equity interest in Liberty Latin America.

[redacted]

In addition to the ARCOS-1 Cable System, [redacted]

B. The Current ARCOS-1 Cable System

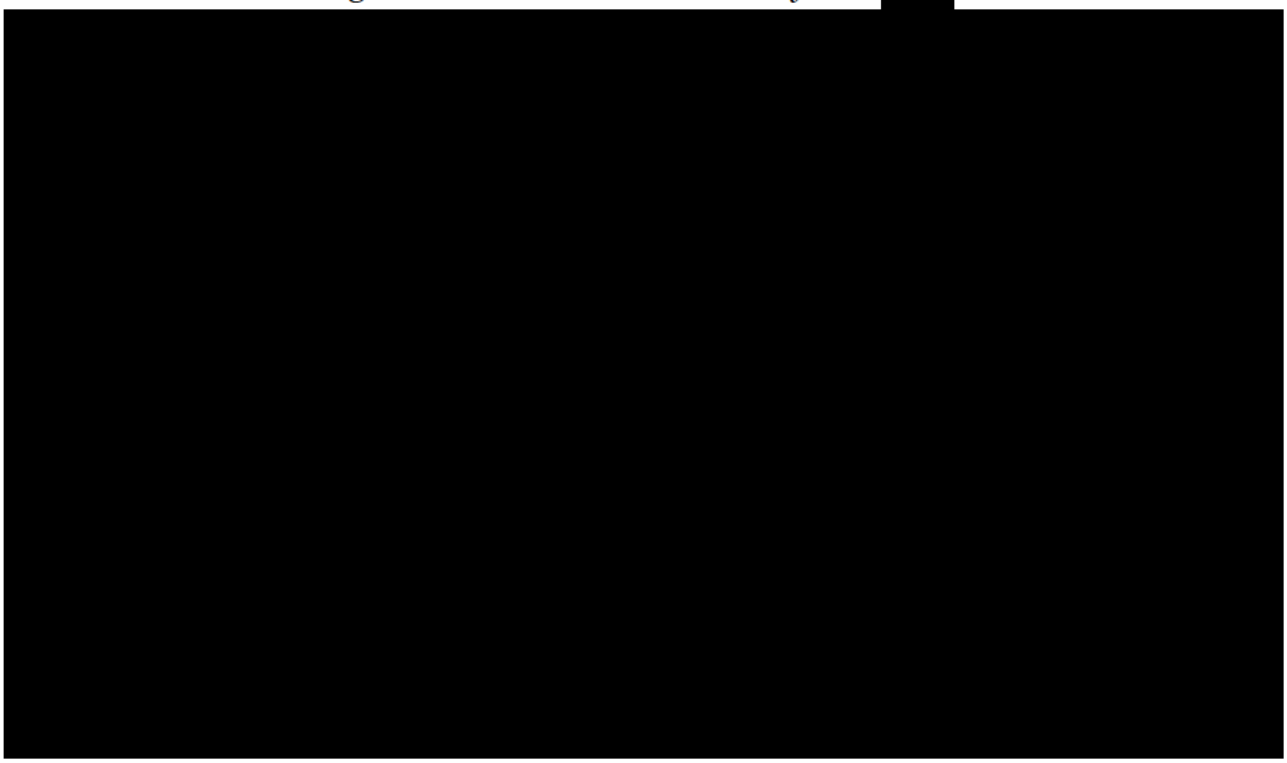
As shown below in Figure 1, the ARCOS-1 Cable System is [redacted] connecting two points in the United States (Miami and Puerto Rico) with landing points across the Caribbean, Latin America, and South America.[23] [redacted]

[22] [redacted]

[23] The landing points are in the Bahamas, Belize, Colombia, Costa Rica, Curacao, the Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, the Turks and Caicos Islands, and Venezuela.

[24] [redacted]

Figure 1: The ARCOS-1 Cable System



C. The Proposed Modification

The proposed modification would establish a new branch to Cuba, landing at Cojimar in Havana, Cuba, as follows.

25

Figure 2: The ARCOS-1 Cable System Cuba Branch Architecture

Figure 3: Data Flows within ARCOS [redacted]

With the addition of Segment 26, the ARCOS-1 Cable System would directly connect the United States to Cuba [redacted]

[redacted]

[26] [redacted]

[redacted]

IV. Procedural Background

The Applicants filed their application with the FCC on October 21, 2021. The FCC referred the application to the Committee on November 26, 2021. The Committee notified the FCC that the Applicants' triage responses were complete on May 5, 2022, starting the 120-day initial review period.

On September 2, 2022, the Committee notified the FCC of its determination that a secondary assessment of the application was warranted because the risk to national security and law enforcement interests cannot be mitigated by standard mitigation measures.[27] The Committee notified the Committee Advisors on September 28, 2022 of its determination to recommend that the FCC deny the application, beginning the 21-day period for the Advisors to oppose the recommendation.[28] No Advisors did so.

V. The Committee Recommends Denying the Application.

The Committee recommends denying the application due to the immitigable risks to the national security and law enforcement interests of the United States.

As FCC Commissioner Starks publicly stated in October 2020, "undersea cables are a critical national security asset," and the FCC "must take a closer look at cables with landing locations in adversary countries."[29] The Government of Cuba has long represented a significant counterintelligence threat to the United States by virtue of its espionage and other intelligence activities targeting the United States. Directly connecting an undersea cable from the United States to Cuba, where a Cuban state-owned company (ETECSA) would have [redacted] control over Segment 26 of the cable's operation and unilateral access to traffic on Segment 26, traffic which would almost certainly include U.S. persons' sensitive information, exacerbates the intelligence risks posed to the United States. This threat is compounded by the Cuban government's relationships with other foreign adversaries, such as the People's Republic of China and the Russian Federation, especially in light of a recently-declassified April 2020 NIC assessment that authoritarian regimes including "China and Russia are improving their ability to analyze and manipulate large quantities of personal information, allowing them to more effectively influence or coerce targets in the United States and allied

---

[27] *See* E.O. 13913 § 5(b), (c).

[28] *See* E.O. 13913 § 9(f).

[29] In the Matter of Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, FCC 20-133, 35 FCC Rcd 10927, 11009 (Oct. 1, 2020) (statement of Comm'r Geoffrey Starks).

countries."[30]

A. The Government of Cuba is a foreign adversary that poses a national security threat to the United States.

1. The Government of Cuba remains a significant counterintelligence threat to the United States.

The United States has long recognized that the Cuban government is a national security threat to the United States. Because of the Cuban government's actions, the United States has imposed some form of economic sanctions on Cuba since the early 1960s, including under the Trading With the Enemy Act of 1917. The Department of Commerce has also identified the Government of Cuba as a foreign adversary for purposes of its authorities to secure the information and communications technology and services supply chain because the Cuban government has "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."[31]

In particular, Cuba has a capable foreign intelligence service with a long history of conducting intelligence operations against the United States. The 2020 National Counterintelligence Strategy specifically recognized the Cuban government's intelligence threat to the United States, noting that, in addition to Russia and the PRC, "[o]ther state adversaries such as Cuba, Iran, and North Korea . . . also pose significant threats" to U.S. counterintelligence efforts. More generally, the NIC has publicly explained that "[a]uthoritarian regimes have developed strong cyber espionage capabilities that enable their influence and coercion operations." As authoritarian regimes "have developed confidence and access, they have begun using tools once reserved for ensuring domestic stability to conduct cyber-attacks and cyber-enabled influence operations against private citizens and organizations in other countries."

A pattern of operations since the end of the Cold War illustrates the Cuban government's efforts in recent decades to steal sensitive information from the United States. In 1998, the FBI arrested 10 individuals in Florida for conducting espionage on the United States on behalf of the Cuban government. The executed search warrants revealed radios, maps, computers, money, and disguises possessed by the spies. The group had tried to infiltrate anti-Castro networks in the United States and spy on U.S. military installations.

Later, in 2001, the FBI arrested Ana Montes, an employee at the Defense Intelligence Agency ("DIA") who had been spying on behalf of the Cuban

---

[30] Office of the Director of National Intelligence, *National Intelligence Council Assessment, (U) Cyber Operations Enabling Expansive Digital Authoritarianism*, at 1, Apr. 7, 2020 (declassified Oct. 5, 2022), NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf (dni.gov).

[31] 15 C.F.R. §§ 7.2, 7.4 (2021); *see* E.O. 13873, 84 Fed. Reg. 22689 (May 15, 2019).

government. Montes was the top Cuba analyst at the DIA and had turned over secrets including the identities of American undercover intelligence officers working in Cuba. She was sentenced to 25 years in prison in 2002.

More recently, in 2010, a U.S. Department of State official and his wife were sentenced to life in prison and 81 months in prison, respectively, for their participation in an espionage conspiracy on behalf of Cuba that spanned three decades. Beginning in 1979, the Cuban Intelligence Service ("CuIS") directed the official (Kendall Myers) to pursue a job with the U.S. government to gain access to classified information. Myers succeeded in getting hired by the State Department's Bureau of Intelligence and Research, where he communicated with CuIS by sending encrypted messages on shortwave radio frequencies and transmitted highly classified national defense information to their handlers through personal meetings and "dead drops."

2. The Government of Cuba is a designated state sponsor of terror.

The Government of Cuba was first designated a state sponsor of terrorism in 1982. At the time, the State Department recognized Cuba's "efforts to promote armed revolution by leftist forces in Latin America" and "groups that use terrorism to undermine existing regimes."[32] Cuba was removed from the State Sponsor of Terrorism List in 2015 after the President certified Cuba had not provided support for international terrorism in the preceding six months.[33] Cuba was designated a state sponsor of terrorism again in January 2021, with the State Department citing Cuba's harboring of fugitives and declining to extradite members of the National Liberation Army (ELN) at Colombia's request.

B. The proposed cable would be under the exclusive control and use of ETECSA, a state-owned entity, that could access U.S. persons' sensitive data and communications to advance the Cuban government's counterintelligence efforts.

1. ETECSA is owned by the Cuban government and subject to its control and direction.

Cuba is an authoritarian state with a centrally planned economy. As part of that centrally planned economy, Cuba's state-owned telecommunications monopoly, ETECSA, appears to be under substantial central ownership and control by the Cuban government. According to the Department of State's Cuba Internet Task Force, "[w]hile it is unclear who ultimately manages and determines ETECSA's

---

[32] *Patterns of International Terrorism: 1982*, United States Dep't of State, 15 (1982), https://www.hsdl.org/?abstract&did=481477.

[33] Karen DeYoung, *Obama removes Cuba from the list of state sponsors of terrorism*, WASH. POST (Apr. 14, 2015), https://www.washingtonpost.com/world/national-security/obama-removes-cuba-from-the-list-of-state-sponsors-of-terrorism/2015/04/14/8f7dbd2e-e2d9-11e4-81ea-0649268f729e_story.html.

policies, a 2011 'Official Gazette' of Cuba's Ministry of Justice reported RAFIN and Banco Financiero Internacional, financial institutions controlled by Cuba's military, owned 27% and 6.2% of its shares, respectively."[34]

For example, ETECSA has taken actions to support the Cuban government's censorship goals. The Government of Cuba uses a combination of website blocking, pressure on website operators, arrests, intimidation, imprisonment, and extralegal surveillance to censor information critical of the regime and to silence its critics. Cuba's Resolution 179/2008 "empowers ETECSA to 'take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics, and morals, as well as the use of applications that affect the integrity or security of the state.'" And ETECSA has used this authority to repress Cuban dissent against the government, including during anti-government protestors in 2020 and 2021—illustrating the Cuban government's direction of ETECSA. As the State Department has explained,

> ETECSA, Cuba's state-owned, monopolistic Internet and telecommunications service provider, has the capability and the legal mandate to open or restrict Internet connectivity at will …. The government often censors text messages that it perceives as subversive. A series of tests conducted by *14ymedio*, an independent digital media outlet in Cuba, confirmed that Cubacel (ETECSA's cell phone provider) had been censoring specific words such as *democracia* (democracy), *dictadura* (dictatorship), and *derechos humanos* (human rights). The Cuban government also blocks voice ports used by the Session Initiation Protocol (SIP), one of the most common protocols used in voice, video, and messaging applications, and any webpage that the Cuban government considers contrary to its interests.

A report from NetBlocks (a British company describing itself as an "[i]ndependent and non-partisan" "global internet monitor") has similarly documented ETECSA's actions in support of the Cuban government's censorship goals. As that report indicates, on networks operated by ETECSA and Cubacel (Cuba's only mobile service provider and an ETECSA subsidiary), social platforms including Twitter, WhatsApp, YouTube, Google, and Facebook were rendered unavailable for several hours during the 2020 and 2021 protests.

---

[34] CUBA INTERNET TASK FORCE: FINAL REPORT, U.S. Dep't of State (June 16, 2019), https://www.state.gov/cuba-internet-task-force-final-report/. Although an Italian firm held a 27% ownership stake in ETECSA until 2011, a different Cuban state-owned firm bought those shares for $706 million; ETECSA has since been fully owned by Cuban state-owned enterprises. Jerrold Colten, *Telecom Italia Sells Etecsa Stake to Rafin SA For $706 Million*, Bloomberg Business (Jan. 31, 2011), http://bloom.bg/1YFxlyo.

2. *Granting the application would present a serious national security risk by giving the Government of Cuba, through ETECSA, the ability and opportunity to access U.S. persons' sensitive data and communications transiting Segment 26.*

If the application is granted as proposed, U.S. persons' internet traffic, data, and communications transiting the proposed ARCOS-1 cable expansion (Segment 26) to Cuba are very likely to be compromised. The Cuban government maintains tight control of Cuban telecommunications networks through ETECSA. ETECSA will be the [redacted] customer using Segment 26 of this cable, based on its status as Cuba's state-owned telecommunications monopoly and the intended [redacted] indefeasible right-of-use agreement between CNL and ETECSA. As practice, all communications transiting Segment 26 of the cable will connect to ETECSA networks. Once on ETECSA networks, they would be vulnerable to interception, misrouting, and other malicious activities that could compromise their confidentiality, integrity, and availability.

Although CNL will own and control the subsea part of the cable and will be the landing party for the landing station in Cojimar, Cuba, [redacted] potentially giving ETECSA direct access to [redacted] other physical equipment located in the CLS. Control of Segment 26 of the ARCOS-1 physical infrastructure in Cuba, in particular, provides opportunities to intercept U.S. persons' communications between Miami and Cuba. The Cuban government could tap connections outside the CLS or use lawful or surreptitious CLS access to install taps inside the CLS.

This risk is not limited to traffic, data, and communications that are destined for Cuba. With the only direct commercial cable connection to the United States, at least three scenarios exist where U.S. traffic, data, and communications intended for destinations *outside* Cuba could nonetheless move through Cuba and be potentially intercepted, regardless of any efforts to filter such traffic.

First, ETECSA could manipulate routing information upstream so that more data transits Cuba instead of other routes, including by offering low-or-no cost transit to small internet providers to entice traffic to transit Segment 26 into Cuba.

Second, ETECSA could use insecurities in internet routing to deliberately mis-advertise Segment 26 as the "best" route for traffic to travel and pull additional traffic across its networks. The internet relies on Border Gateway Protocol ("BGP"), which enables network providers to share information about traffic routing so that they can identify the "best" routes for traffic to reach its destination. BGP, designed at a time when networks were assumed to be trusted, suffers from fundamental vulnerabilities. As each of the Committee members has publicly explained in other FCC proceedings, these vulnerabilities facilitate the misrouting of and access to

traffic, data, and communications, and create national security risks of espionage, theft, and sabotage by foreign adversaries.[35] Foreign adversaries and telecommunication providers subject to their direction or control (like ETECSA) can use BGP vulnerabilities to gain access to sensitive data and communications. For example, when the FCC revoked China Telecom Americas' ("CTA") section 214 license, the record showed that BGP vulnerabilities facilitated CTA's misrouting of U.S. traffic to the PRC on numerous occasions between 2010 and 2019, and thus provided a foreign adversary with opportunities to disrupt, capture, examine, and alter U.S. traffic.[36] Similarly, Russian telecommunications providers have hijacked and redirected traffic by exploiting BGP vulnerabilities.[37] ETECSA could also take advantage of these vulnerabilities to cause BGP route leaks, leading traffic not destined for Cuba to be misrouted over Segment 26 and into the Cuban government's hands.

Third, if another undersea cable to destinations in Latin America or the Caribbean is severed or disrupted (whether through deliberate or malicious activity, natural disaster, or inadvertence), the overflow traffic could re-route through Cuba via Segment 26 on its way to its final destination.

These risks of increased access by the Cuban government to U.S. persons' internet traffic, data, and communications (whether destined for Cuba or not) are serious national security concerns because they would make the Cuban government an even greater counterintelligence threat to the United States. Increased collection of U.S. persons' data and communications could greatly assist the CuIS in its intelligence endeavors against the United States. The U.S. Intelligence Community has also warned of the capabilities that a foreign adversary may gain with access to large volumes of U.S. persons' data. In July 2015, then-Director of the National Security Agency Admiral Michael Rogers stated that "we need to recognize that increasingly data has a value all its own[.]"[38] With big-data analytics, he explained, a foreign adversary could gain intelligence insights useful for targeting U.S. persons; for example, the foreign adversary might know whether a U.S. person traveling to a foreign country was just a tourist or had other reasons

---

[35] *See* Letter from Matthew G. Olsen, Assistant Attorney General for National Security, U.S. Department of Justice, and William A. LaPlante, Under Secretary of Defense, Acquisition & Sustainment, U.S. Department of Defense, to Marlene H. Dortch, Secretary, FCC, *Re: In the Matter of Secure Internet Routing*, PS Docket 22-90 (F.C.C. Sept. 14, 2022) ("DOJ and DOD Comments on Secure Internet Routing"); Reply Comments of the Cybersecurity and Infrastructure Agency, *In the Matter of Secure Internet Routing*, PS Docket 22-90 (F.C.C. July 7, 2022) ("CISA Comments on Secure Internet Routing").

[36] *See* DOJ and DOD Comments on Secure Internet Routing, *supra* note 34, at 3–4; *In the Matter of China Telecom (Americas) Corporation*, Order on Revocation and Termination, 2021 WL 516884, 56–64 (2021).

[37] *See* CISA Comments on Secure Internet Routing, *supra* note 35, at 2–3.

[38] Exhibit 115 at EB-PUBLIC-2018, *Beyond the Build: Leveraging the Cyber Mission Force,* Aspen Institute (July 23, 2015) (Transcript of statement by Adm. M. Rogers), http://aspensecurityforum.org/wp-content/uploads/2015/07/Beyond-the-Build-Leveraging-the-Cyber-Mission-Force.pdf.

for travel.[39] The White House's National Security Strategy recently recognized this risk, which states that the United States "must ensure strategic competitors cannot exploit foundational American and allied technologies, know-how, or data to undermine American and allied security."[40] These concerns provide additional background for the Committee's concerns, as a subsea cable like the ARCOS-1 Cable System landing in Cuba would provide additional opportunities for Cuban government to collect U.S. communications and data traffic for further big-data analysis (by themselves or their allies, as discussed below).

Importantly, [redacted] thus cannot adequately mitigate these risks with respect to traffic not bound for Cuba.

[39] *Id.* at EB-PUBLIC-2018 to -19.

[40] NATIONAL SECURITY STRATEGY, The White House (October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[41] The OSI model is a technical standard defining seven layers of activity that computer systems use to communicate over a network. Introduced in 1983, it was adopted by the International Organization for Standards in 1984 and is widely adopted by telecommunications and information technology and services companies to help visualize and describe how networks operate. Its seven layers are (1) physical, (2) data link, (3) network, (4) transport, (5) session, (6) presentation, and (7) application.

[42] [redacted]

C. The Cuban government's relationship with the PRC heightens the national security threat to the United States.

1. Cuba maintains a strong relationship with the PRC.

In recent years, Cuba has maintained strong ties to the PRC in economic, diplomatic, and military dimensions.[43] The State Department explained in an unclassified report to Congress in July of this year that "Cuba and the PRC have collaborated for six decades, including coordinated messaging and a close party-party relationship. President Xi Jinping visited Cuba in 2014. Cuban President Miguel Diaz-Canel included the PRC on his first international trip overseas as President in 2018."[44] As the PRC remains the most sophisticated counterintelligence and cyber threat to the United States, this strong relationship between the Cuban government and the PRC heightens the concerns described above to the extent that this relationship results in the Government of Cuba sharing any information it collects through the ARCOS-1 cable with the PRC and its intelligence services. In 2018, *The Diplomat* noted that the Cuban government has, for instance, reportedly been known to sell its intercept data from U.S. communications to third-party buyers, particularly military adversaries of the United States including China.[45]

The PRC has boasted of its "strong and growing political, diplomatic, and military ties to authoritarian governments in Cuba and Nicaragua."[46] The relationship between the PRC and Cuba's militaries is characterized by technical assistance programs, and senior-level meetings between the PRC's and Cuba's military.[47] For example, the Vice-Chairman of China's Central Military Commission received the Chief of Staff of Cuba's military in September 2019, where he pledged an expansion of military exchanges.[48]

Strong military ties between the Cuban government and the PRC is even

---

[43] *See generally* Diana Roy, *China's Growing Influence in Latin America*, Council on Foreign Relations (Apr. 12, 2022), https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri.

[44] U.S. Dep't of State, Congressional Report Transmittal Letter, Report to Congress on Efforts by the People's Republic of China to Expand its Presence and Influence in Latin America and the Caribbean, P.L. 117-81, at 3 (2022) ("State Department Congressional Report on China in Latin America and the Caribbean").

[45] Victor R. Lee, *Satellite Images: A (Worrying) Cuban Mystery*. THE DIPLOMAT. https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery/.

[46] State Department Congressional Report on China in Latin America and the Caribbean, *supra* note 44, at 3.

[47] U.S.-China Economic and Security Review Commission, *China's Engagement with Latin America and the Caribbean*, https://www.uscc.gov/sites/default/files/Research/China's%20Engagement%20with%20Latin%20America%20and%20the%20Caribbean_.pdf.

[48] State Department Congressional Report on China in Latin America and the Caribbean, *supra* note 44, at 2.

more apparent through the physical presence of Chinese military personnel on the island of Cuba itself. According to an October 2018 staff report of the U.S.-China Economic and Security Review Commission, the PRC maintains physical presences at Soviet-era intelligence facilities at Bejucal in what appears to be a signals intelligence ("SIGINT") collection operation.[49] The installation near Bejucal has been previously used to intercept electronic communications from the United States, and commercial satellite images of the intelligence collection base from 2018 show a marked change in the size and sophistication of the antennas used for SIGINT collection, which indicates a high level of economic investment.[50]

Additionally, China is now Cuba's largest trading partner[51] and, as one of Cuba's main creditor nations, reportedly wrote off $6 billion of Cuba's debt in 2011.[52] In 2018, Cuba formally signed a memorandum of understanding to join China's Belt and Road Initiative.[53] Since then, Chinese corporations have

---

[49] U.S.-China Economic and Security Review Commission, *China's Engagement with Latin America and the Caribbean*, *supra* note 47.

[50] Lee, Satellite Images: A (Worrying) Cuban Mystery, *supra* note 45.

[51] Marc Frank, *Cuba's imports from China slump 40% in 2020, extending long decline*, REUTERS (Feb. 5, 2021), https://www.reuters.com/article/cuba-china-trade/cubas-imports-from-china-slump-40-in-2020-extending-long-decline-idUSL1N2K919P.

[52] Kenneth Rapoza, *China Has Forgiven Nearly $10 Billion in Debt. Cuba Accounts for Over Half*, FORBES (May 29, 2019), https://www.forbes.com/sites/kenrapoza/2019/05/29/china-has-forgiven-nearly-10-billion-in-debt-cuba-accounts-for-over-half/?sh=ac83e66615ba.

[53] Scott Foster, *Belt & Road encircles Latin America and the Caribbean*, ASIA TIMES (Jan. 8, 2022), https://asiatimes.com/2022/01/belt-road-encircles-latin-america-and-the-caribbean/. Since 2013, the PRC government has made massive infrastructure investments through the One Belt, One Road ("OBOR") initiative. Exhibit 27 at EB-PUBLIC-559 to -566, 2018 Report to Congress of the U.S.-China Economic and Security Review Commission, at 259 115th Cong.(2018) (Chapter 3, Section 1: Belt and Road Initiative and Digital Silk Road), https://www.uscc.gov/sites/default/files/2019-09/2018%20Annual%20Report%20to%20Congress.pdf. Although initially focused on traditional physical infrastructure projects ostensibly directed toward economic goals, the OBOR initiative has more recently pivoted to cyberspace through the Digital Silk Road initiative. *Id.* at EB-PUBLIC-564. The OBOR and Digital Silk Road initiatives are aimed at connecting the world through a web of PRC-funded infrastructure. *Id.* at EB-PUBLIC-559; Exhibit 28 at EB-PUBLIC-605, D. Kliman and A. Grace, *Power Play: Addressing China's Belt and Road Strategy*, Center for a New American Security 1 (Sept. 2018) (Executive Summary), https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Power-Play-Addressing-Chinas-Belt-and-Road-Strategy.pdf?mtime=20180920093003*; see also* Exhibit 29 at EB-PUBLIC-664 to -665, *Assessment on U.S. Defense Implications of China's Expanding Global Access,* U.S. Dep't of Defense 12 (Dec. 2018). Digital infrastructure investments have become increasingly important for the PRC government's goal of turning China into a "cyber superpower." Exhibit 30 at EB-PUBLIC-682, DigiChina, *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference,* New America (last visited Mar. 9, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/*; see also* Exhibit 28 at EB-PUBLIC-614 ("The Belt and Road [another translation of One Belt, One Road] is advancing Beijing's intention to become the world's leading information technology power.") And controlling the flow of data becomes increasingly important for shifting the balance of geopolitical power in China's favor.

participated in infrastructure projects in Cuba's energy sector[54] and in Cuban commercial ports.[55] In December 2021, Cuba expanded its involvement in the Belt and Road Initiative by signing an even broader memorandum of understanding with China to further promote construction initiatives.[56]

Chinese actors have been especially active in Cuba's telecommunications sector; indeed, as reported in *The Diplomat*, "Chinese companies have played a key part in building Cuba's telecommunications infrastructure, a system the regime uses to control its people, just as the Chinese Communist Party (CCP) does within its own borders."[57] Chinese companies partly financed the ALBA-1 undersea cable linking Cuba to Venezuela.[58] As the State Department recently reported to Congress, "Cuba's state telecommunications monopoly ETECSA primarily uses equipment from PRC tech providers."[59] Citing ETECSA's own corporate magazine, the Institute for War and Peace Reporting found that ETECSA's three primary technology providers include the Chinese companies Huawei and ZTE[60]—companies that the United States has repeatedly recognized as presenting national security concerns precisely because their equipment provides the means for the PRC to access the data, communications, and equipment that traverse it.[61] Other open-

---

Exhibit 30 at EB-PUBLIC-682, DigiChina, *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference,* New America (last visited Mar. 9, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/*; see also* Exhibit 28 at EB-PUBLIC-614 ("The Belt and Road [another translation of One Belt, One Road] is advancing Beijing's intention to become the world's leading information technology power."). While such investments alone may not cause concern, the combination of this objective with the state-sponsored theft of U.S. persons' data and targeted acquisitions of U.S. companies with sensitive personal data paints a different, more troubling picture.

54 Matthew Crittenden et al., *China's BRI in Latin America: Case Study—Sustainable Energy in Cuba*, TEARLINE.MIL (Aug. 14, 2020), https://www.tearline.mil/public_page/china-bri-in-caribbean_energy/.

55 Marc Frank, *China piles into Cuba as Venezuela fades and Trump looms*, REUTERS (Feb. 14, 2017), https://www.reuters.com/article/us-cuba-china-analysis/china-piles-into-cuba-as-venezuela-fades-and-trump-looms-idUSKBN15T2PE.

56 State Department Congressional Report on China in Latin America and the Caribbean, at 3, *supra* note 44.

57 Leland Lazarus and Evan Ellis, *How China Helps the Cuban Regime Stay Afloat and Shut Down Protests* (Aug. 3, 2021), THE DIPLOMAT, https://thediplomat.com/202/08/how-china-helps-the-cuban-regime-stay-afloat-and-shut-down-protests/.

58 *See* Larry Press, *China Wins First Round of Cuban Internet Investment*, A NEW DOMAIN (2015), https://anewdomain.net/china-wins-first-round-cuban-internet-investment-analysis/.

59 State Department Congressional Report on China in Latin America and the Caribbean, *supra* note 44, at 3.

60 Claudia Padron Cueto, *Cuba's Internet: Blocked Pages and Chinese Tech*, INSTITUTE FOR WAR & PEACE REPORTING (Dec. 18, 2020), https://iwpr.net/global-voices/cubas-internet-blocked-pages-and-chinese-tech.

61 *See*, *e.g.*, Pub. L. 115-232, 132 Stat. 1917 (Aug. 13, 2018), § 889 (codified at 41 U.S.C. note prec.

source information reports Huawei signed a contract with the Cuban government in 2000 to set up fiber optic cables throughout Cuba,[62] and that Huawei is operating fiber optic home internet connections in Cuba for ETECSA.[63] The Swedish civil society group Qurium wrote in a 2020 report that it had detected Huawei network management software on the Cuban internet.[64] These commercial connections are particularly concerning in light of the NIC's partially declassified April 2020 assessment of the threat posed by Chinese cyber operations:

> Beijing will have increasing opportunities to use commercial channels to exert its digital authoritarianism in the next few years. Beijing will be able to exploit Chinese companies' expansion of telecommunications infrastructure and digital services, these enterprises' growing presence in the daily lives of populations worldwide, and Beijing's rising global economic and political influence.[65]

2. The potential for the PRC to obtain increased sensitive U.S.-person information presents significant concern.

Given these close relations between the PRC and the Cuban government, the possibility that PRC intelligence services could gain increased access to the sensitive personal information of millions of U.S. persons—whether via the Cuban government or Chinese companies working in the Cuban telecommunications sector—further heightens the national security risks posed by this application. The 2017 Equifax data breach, for example, helps demonstrate the significant threat posed by the PRC's acquisition of U.S. person data. In February 2020, DOJ announced an indictment of PRC military hackers for their alleged role in the 2017 Equifax data breach, calling the scale of the PRC government's data theft "staggering."[66] The Equifax indictment charged four members of the PRC

---

§ 3901); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020).

[62] Lazarus and Ellis, How China Helps the Cuban Regime Stay Afloat and Shut Down Protests, *supra* note 57.

[63] *Cuba announces launch of broadband home internet*, CBS News (Jan. 31, 2016), https://www.cbsnews.com/news/cuba-announces-launch-of-broadband-home-internet/.

[64] Jamie Moreno, *China Seen Backing 'Digital Authoritarianism' in Latin America*, VOA (Jan 14, 2022), https://www.voanews.com/a/china-seen-backing-digital-authoritarianism-in-latin-america-/6398072.html.

[65] National Intelligence Council Assessment, (U) Cyber Operations Enabling Expansive Digital Authoritarianism, *supra* note 30, at 4.

[66] Exhibit 15 at EB-PUBLIC-111, *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (Feb. 10, 2020)

government's People's Liberation Army with hacking into the computer systems of credit-reporting agency Equifax and thereby stealing the sensitive personal information of 145 million Americans—nearly half of all American citizens.[67] According to the then-Attorney General, the Equifax breach presented a continuing pattern of "China's voracious appetite for the personal data of Americans," including the theft of personnel records from the U.S. Office of Personnel Management, and the intrusion into the Anthem health insurance company.[68]

In announcing the Equifax indictment, the then-Attorney General explained that the stolen data not only had economic value but could also "feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages."[69] The proposed cable compounds that risk. The Cuban government could soon glean communications, travel records, health records, credit information, and any other information transiting Segment 26, and share that information with the PRC for use in its data-analytics efforts described in the NIC's April 2020 threat assessment. By combining whatever information the Cuban government gleans from Segment 26 with the personnel data that the PRC has already obtained, PRC intelligence services may have the capability to augment a database more detailed than any nation has ever possessed about one of its rivals.[70] And the NIC further explained that Beijing's "access to personal data of other countries' citizens, along with AI-driven analytics, will enable it to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship" as well as other means of coercion.[71]

In other similar national security contexts, Congress, through recent legislation, and the Executive Branch have recognized the threat posed by

---

(hereinafter Barr Announcement), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military; Exhibit 17 at EB-PUBLIC-136, *United States v. Wu Zhiyong et al.*, No. 20-cr-046, Indictment (N.D. Georgia filed Jan. 28, 2020); Exhibit 14 at EB-PUBLIC-108, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*, U.S. Dep't of Justice (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

67 Exhibit 15 at EB-PUBLIC-111, *Barr Announcement*; Exhibit 17 at EB-PUBLIC-137.

68 Exhibit 15 at EB-PUBLIC-111, *Barr Announcement*.

69 Exhibit 15 at EB-PUBLIC-111.

70 *See, e.g.,* Exhibit 22 at EB-PUBLIC-428, Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired (Feb. 11, 2020), https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/; Exhibit 23 at EB-PUBLIC-432, Ben Kochman, *Equifax Hack Shows China's Expanding Hunger for Data*, Law360 (Feb. 11, 2020), https://www.law360.com/cybersecurity-privacy/articles/1242594/equifax-hack-shows-china-s-expanding-hunger-for-data ("China is building a digital dossier on individual American citizens. [ ] And through this one [Equifax] breach alone, they built half of that dossier."). *See also* Exhibit 21 at EB-PUBLIC-422, David Sanger, *Marriott Concedes 5 Million Passport Numbers lost to Hackers Were Not Encrypted,* New York Times (Jan. 4, 2019), https://www.nytimes.com/2019/01/04/us/politics/marriott-hack-passports.html.

71 See National Intelligence Council Assessment, (U) Cyber Operations Enabling Expansive Digital Authoritarianism, *supra* note 30, at 3–4.

potentially increased PRC access to sensitive personal data collected and maintained by U.S. companies. For example, in August 2018, Congress responded to shifts in the national security landscape and resulting concerns that PRC investments could enable access to U.S. companies' sensitive personal data in ways that threaten national security by passing the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA").[72] FIRRMA broadened the scope of the Committee on Foreign Investment in the United States ("CFIUS")'s authority to include non-controlling foreign investments in a U.S. business that "maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[73] And FIRRMA urged CFIUS to examine, in all transactions under its review, whether they are likely to expose "personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security."[74]

The regulations implementing FIRRMA spelled out these concerns. For example, the FIRRMA regulations recognized that foreign access to certain types of financial data raise national security concerns if the data could be used to target individuals vulnerable due to financial hardship.[75] Likewise, foreign access to collections of personal insurance information, health-related data, nonpublic electronic communications, geolocation data, biometric identification data, government identification or security clearance information, and genetic information could also threaten national security.[76]

The Executive Branch has consistently recognized the importance of protecting U.S. persons' data, communications, and information from access by the PRC and other foreign adversaries. In June 2021, the President issued E.O. 14034, "Protecting Americans' Sensitive Data From Foreign Adversaries,"[77] and in September 2022, E.O. 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States."[78] As the latter explains, because "[d]ata is an increasingly powerful tool for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security," CFIUS must consider whether and how transactions involving access to U.S. persons' data may constitute a threat

---

[72] Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, §§ 1702–1728, 132 Stat. 2174–2207 (2018).

[73] *Id.* § 1703(a)(4)(B)(iii)(III), 132 Stat. 2178.

[74] FIRRMA, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2176–77.

[75] *See CFIUS Final Rule*, 85 Fed. Reg. at 3132–33 (final definition of sensitive personal data); *CFIUS Proposed Rule*, 84 Fed. Reg. at 50178.

[76] *See CFIUS Final Rule*, 85 Fed. Reg. at 3132.

[77] E.O. 14024, 86 Fed. Reg. 31423 (June 9, 2021).

[78] E.O. 14083 § 3(c), 87 Fed. Reg. 57369 (Sept. 20, 2022).

to national security.[79]

The FCC has also recognized the importance of preventing PRC access to U.S. persons' traffic, data, and communications through the ownership and operation of subsea cables. For example, in granting Google's and Facebook's application for a license to own and operate the Pacific Light Cable Network system connecting the United States, Taiwan, and the Philippines, the FCC agreed with and accepted the Committee's recommendation to condition the license on the companies' compliance with, among other things, provisions to protect data as it transits the cable system.[80] That was only after the Committee objected to an earlier configuration in which the cable system would have directly connected to Hong Kong and been partially owned and operated by an entity with ties to the PRC government.[81] As detailed by the Committee's recommendation to partially deny the application, the PRC government has made sustained efforts to acquire the sensitive personal data of millions of U.S. persons—including through the PRC government's access to other countries' data through digital infrastructure investments and other relationships.[82]

D. The Cuban government's relationship with the Russian Federation heightens the national security threats to the United States.

The Cuban government's longstanding and expansive relationship with the Russian Federation similarly enhances the risks of foreign-adversary access to U.S. person' traffic, data, and communications. As the Office of the Director of National Intelligence described in the most recent Annual Threat Assessment of the U.S. Intelligence Community, Russia has "supported Cuba" as part of broader strategy to "expand its global military, intelligence, security, commercial, and energy footprint and build partnerships aimed at undermining U.S. influence and boosting its own."[83] While Cuban-Russian relations are less than their peak of interdependence during the Cold War, in recent years the two countries have again seen warming relations. In 2014, Russia wrote off 90% of Cuba's $35 billion in debt to the Soviet

---

79 *Id.*

80 Press Release, The United States Department of Justice, *Team Telecom Recommends FCC Grant Google and Meta licenses for Undersea Cable* (Dec. 17, 2021) https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable ("PLCN Press Release"); *see also* Actions Taken Under the Cable Landing License Act, FCC Public Notice, DA No. 22-41, GU Holdings Inc., SCL-LIC-20200827-00038 (Jan. 26, 2022).

81 Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network (PLCN), *In the Matter of GU Holdings Inc., Edge Cable Holdings USA, LLC and Pacific Light Data Communication Co. Ltd.*, (F.C.C. June 17, 2020).

82 *Id.*

83 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* 10 (Feb. 2022), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Union, an event that marked the start of the contemporary friendly era;[84] since then, Russia has further postponed payments until 2027.[85] Cuba and Russia have greatly expanded their economic relationship, with trade volumes doubling between 2013 and 2019.[86] In 2021, Cuban and Russian leaders signaled their intention to strengthen the countries' "strategic partnership."[87]

Most recently, the Cuban foreign ministry and state media outlets adopted Russian narratives surrounding the war in Ukraine by downplaying the conflict, adopting the official Russian framing of a "special military operation," and criticizing U.S.-imposed sanctions on Russia.[88] The Cuban government has imported more than $322 million worth of oil from Russia since Russia invaded Ukraine—the largest quantity since the collapse of the Soviet Union—providing another market for Russian oil, helping Russia reduce the effect of international sanctions, and facilitating Russia's continued invasion of Ukraine.[89]

Cuba and Russia have also had some publicly reported collaboration in the telecommunications space. In 2020, the ministers of communications for both countries met to discuss collaboration on "telecommunications, digital television, the Internet, and cybersecurity," according to Cuban state media.[90] In 2019, a delegation of Russian government and business leaders, including representatives of the U.S.-sanctioned Russian defense conglomerate Rostec, visited Cuba to discuss collaboration in cybersecurity and digital trade.[91] As a result of that visit, the

---

84 Andrey Ostroukh and Jose do Cordoba, *Russia Writes off Cuba Debt*, WALL ST. J. (Jul. 12, 2014), https://www.wsj.com/articles/russia-writes-off-cuba-debt-1405083869.

85 Polina Devitt and Dave Sherwood, *Russia postpones Cuba debt payments amid warming relations*, REUTERS (Feb. 22, 2022), https://www.reuters.com/markets/europe/russia-postpones-cuba-debt-payments-amid-warming-relations-2022-02-23/.

86 Andrea Rodriguez, *As US turns its back on Cuba, Russia steps in*, CHRISTIAN SCIENCE MONITOR (Oct. 29, 2019), https://www.csmonitor.com/World/Americas/2019/1029/As-US-turns-its-back-on-Cuba-Russia-steps-in.

87 *Russia, Cuba Seek Closer 'Strategic Partnership'*, FRANCE24 (Apr. 20, 2021), https://www.france24.com/en/live-news/20210420-russia-cuba-seek-closer-strategic-partnership.

88 Graham Keeley, *Cuba Adopts Russian Narrative on Ukraine War*, VOA (Apr. 7, 2022), https://www.voanews.com/a/cuba-adopts-russian-narrative-on-ukraine-war-/6519782.html; Dave Sherwood, *Russia ally Cuba slams U.S. over Ukraine crisis, urges diplomacy*, REUTERS (Feb. 23, 2022), https://www.reuters.com/markets/europe/russia-ally-cuba-slams-us-over-ukraine-crisis-urges-diplomacy-2022-02-23/; Dave Sherwood, *Cuba to deepen ties with Russia as Ukraine tensions mount*, REUTERS (Feb. 19, 2022), https://www.reuters.com/world/americas/cuba-deepen-ties-with-russia-ukraine-tensions-mount-2022-02-19/.

89 Nora Gámez Torres, *Cuba ramps up imports of Russian oil, helping Putin to evade sanctions*, MIAMI HERALD (Oct. 17, 2022), https://www.miamiherald.com/news/nation-world/world/americas/cuba/article267329272.html.

90 Jorge Ruiz Miyares, *Cuba and Russia assess cooperation in the field of communications*, RADIO HABANA CUBA A(Feb. 13, 2020), https://www.radiohc.cu/en/noticias/nacionales/214325-cuba-and-russia-assess-cooperation-in-the-field-of-communications.

91 Russia, Cuba agree to boost cooperation in cyber-security and communications, TASS (Mar. 27,

Cuban government and the Russian government signed a memorandum of understanding to "strengthen cooperation in the sphere of telecommunications"—including by testing Russian-made information technology and communications equipment for use by the Cuban government to store and handle data in Cuban territory.[92]

More generally, Russia (like China) is "using digital authoritarian capabilities to aid their allies and are allowing their firms to sell equipment and know-how on the open market."[93] "Firms around the world sell capabilities and expertise that facilitate governments' internal and extraterritorial monitoring and repression."[94]As the NIC has explained in its partially declassified April 2020 assessment, Russia's acquisition of U.S. persons' sensitive data poses a risk to national security. Russia, like China, is "improving [its] ability to analyze and manipulate large quantities of personal information," enabling it "to more effectively influence or coerce targets in the United States or allied countries."[95] And Russia, like China, engages in "cyber espionage efforts [that] have helped [it] acquire bulk data" such as in 2013 when the Russian Federal Security Service "sponsored a theft of 3 billion accounts from a U.S. web services company."[96]

VI. Conclusion

Although the United States supports the Cuban people's access to an open, interoperable, secure, and reliable internet, this particular license application pertains to a cable landing that presents immitigable risk to U.S. national security and law enforcement interests. By landing a subsea cable in Cuban territory, the Government of Cuba would be well positioned to collect all U.S. persons' communications and sensitive data traversing Segment 26 the cable. Given the significant counterintelligence threat that the Government of Cuba presents to the United States and its close relationships with the PRC, Russia, and other foreign adversaries, this application presents an unacceptable and immitigable risk to U.S. national security and law enforcement interests. Accordingly, the Committee recommends that the FCC deny the Applicants' request to modify the ARCOS-1 cable-landing license application.

2019), https://tass.com/world/1050789; see Press Release, U.S. Treasury Sanctions Nearly 100 Targets in Putin's War Machine, Prohibits Russian Gold Imports, U.S. Dep't of the Treasury (June 28, 2022), https://home.treasury.gov/news/press-releases/jy0838.

92 Russia, Cuba agree to boost cooperation in cyber-security and communications, *supra* note 91.

93 National Intelligence Council Assessment, (U) Cyber Operations Enabling Expansive Digital Authoritarianism, *supra* note 30, at at 5.

94 *Id.* at 6.

95 *Id.* at 1, 3.

96 *Id.* at 4.

November 29, 2022

Respectfully submitted:

STEPHANIE WEINER

Digitally signed by STEPHANIE WEINER
Date: 2022.11.29 19:04:57 -05'00'

Stephanie Weiner
Chief Counsel (Acting),
National Telecommunications and
Information Administration
U.S. Department of Commerce, Rm. 4713
1401 Constitution Ave., N.W.
Washington, D.C. 20230
(202) 482-1816

On behalf of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector