Congress of the United States
House of Representatives
Washington, DC 20515-0906

July 21, 2025

Mr. Sundar Pichai
Chief Executive Officer
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Mr. Satya Nadella
Chairman and Chief Executive Officer
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Mr. Mark Zuckerberg
Chief Executive Officer
Meta Platforms, Inc.
1 Hacker Way
Menlo Park, CA 94025

Mr. Matt Garman
Chief Executive Officer
Amazon Web Services, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Pichai, Mr. Nadella, Mr. Zuckerberg, and Mr. Garman:

Resting on the ocean floor, submarine telecommunications cables, often referred to as "subsea cables," form one of the most strategically significant, and increasingly vulnerable, components of the world's digital infrastructure. Subsea cables transmit over 95 percent of intercontinental data, powering not only global commerce and innovation but also the core operational systems of national security, intelligence, and defense.[1] Their uninterrupted function is essential to your companies' platforms and to the communications systems upon which the U.S. government and its allies rely daily.

As co-owners, consortium members, service integrators, or critical end-users, your companies play a central role in the functionality, resilience, and security of these systems. As such, your participation is essential to ongoing congressional oversight efforts examining the extent to which foreign adversarial actors are positioning themselves, both overtly and covertly, to compromise subsea cable systems at key points of vulnerability. These efforts are being jointly led by the House Committee on Homeland Security's Subcommittee on Transportation and Maritime Security, the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, and the House Foreign Affairs Committee's Subcommittee on Europe ("the Committees").

A growing body of evidence points to a pattern of coordinated malign activity linked to the People's Republic of China (PRC) and the Russian Federation targeting subsea infrastructure

[1] Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, "*Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*," (August 16, 2024), CSIS, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

in the Baltic Sea, Indo-Pacific, and other strategic regions.[2] In the Baltic Sea, multiple sabotage incidents in recent years have been attributed to commercial vessels whose flag registration, beneficial ownership, or operational control are traceable to PRC or Russian interests.[3] These vessels have engaged in deliberate anchor-dragging, transponder disablement, and irregular navigational behavior in proximity to high-value subsea cables, which are tactics consistent with grey-zone operations designed to exploit legal ambiguity and avoid direct attribution.[4]

A similar pattern has emerged in the Indo-Pacific. Targeted disruptions near Taiwan in 2023 and again in 2025 severed the island's connectivity to critical regional and global networks.[5] The implicated vessels operated under obscured ownership and were staffed by PRC nationals.[6] These cases, like those in the Baltic, demonstrate an increasingly brazen strategy to physically degrade subsea infrastructure while evading the traditional triggers of armed conflict under international law.

However, the vulnerabilities facing subsea cable systems extend beyond physical sabotage. At the same time that maritime disruptions are occurring globally, PRC-affiliated firms have steadily gained "legitimate" access to the construction, maintenance, and repair of subsea cable systems through commercial partnerships, multinational consortia, and state-backed investment. Entities such as S.B. Submarine Systems (SBSS), a maintenance provider majority-owned by China Telecom, illustrate how Beijing is embedding itself in the very architecture it may seek to surveil, degrade, or control.

This dual-pronged strategy, combining grey-zone interference with lawful integration into the subsea cable supply chain, poses a long-term risk to the integrity and resilience of global communications, financial networks, and the operation of cloud-based government and commercial services. The same foreign adversarial actors engaged in sabotage at sea may also be positioned to exploit privileged access to subsea cable segments, landing stations, or terminal equipment under the cover of routine commercial servicing. This convergence of physical and institutional access represents an evolving threat vector that warrants proactive scrutiny by both the U.S. government and the private sector.

In recognition of these threats, the Federal Communications Commission (FCC) recently announced its intention to vote on a rule in early August 2025 prohibiting the use of PRC-

---

[2] Jack Burnham, "*US and allies must get tough on Russia, China's deep-sea cable sabotage*," (February 27, 2025), New York Post, https://www.fdd.org/analysis/op_eds/2025/02/27/us-and-allies-must-get-tough-on-russia-chinas-deep-sea-cable-sabotage/.
[3] Erik Brown, "*The Baltic Sea at a Boil: Connecting the Shadow Fleet and Episodes of Subsea Infrastructure Sabotage*," (June 5, 2025), Carnegie Endowment for Int. Peace, https://carnegieendowment.org/research/2025/06/baltic-russia-maritime-cable-sabotage?lang=en.
[4] *Id*.
[5] Timothy Boyle, "*A New Strategy to Counter Chinese Sabotage of Taiwan's Undersea Cables*," (May 20, 2025), Just Security, https://www.justsecurity.org/113221/chinas-shadow-fleet-war-on-taiwans-undersea-cables/.
[6] *Id*.

manufactured technology and equipment in any subsea cable landing in the United States.[7] Once adopted, this rule will prevent entities that utilize restricted PRC components from receiving licenses to build or operate cables that land in the U.S., and from leasing capacity on cables operated by others.[8] The FCC's action represents a critical step in closing gaps that have allowed adversarial actors, particularly from the PRC, to embed themselves in core segments of U.S.-connected subsea cable systems.

Amid these risks, the Committees are examining whether leading U.S. technology firms have adopted adequate safeguards to mitigate exposure to adversarial entities involved in subsea cable operations. We are particularly concerned by the possibility that entities affiliated with the PRC, such as SBSS, Huawei Marine, China Telecom, and China Unicom, have continued to provide maintenance or servicing to cable systems in which your companies maintain direct or indirect operational involvement or ownership.

Congressional oversight of these matters is essential to ensuring that foreign access to subsea cable infrastructure does not become a backdoor for espionage, disruption, or exploitation of U.S. data and communications assets. To support the Committees' investigation, we request that each company submit a separate written response no later than 5:00 p.m. on August 4, 2025, addressing the inquiries and information requests outlined below. Each response should encompass all relevant entities under your corporate structure, including parent companies, subsidiaries, affiliates, joint ventures, consortia, and any special purpose vehicles operating on your behalf or under your direction.

1. Please identify each subsea cable system in which your company, its subsidiaries, or controlled affiliates hold any form of ownership interest, voting authority, financial stake, or operational role, including participation through consortia, joint ventures, or special purpose vehicles.
    a. For each subsea cable system, please provide the system name, geographic landing points, current operational status, total design capacity, and the identity of all co-owners and cable landing station operators.
    b. Additionally, for each identified subsea cable system, please confirm whether any technology, hardware components, or system elements of PRC origin, whether manufactured, integrated, maintained, or otherwise serviced by PRC-affiliated entities, are currently deployed, embedded, or utilized at any point in the system's infrastructure. This includes, but is not limited to, optical amplifiers, repeaters, branching units, terminal equipment, cable landing station hardware, or network management systems. If such components are present, please identify the specific items, their function within the system, and the name(s) of the vendors or service providers involved.

---

[7] David Shepardson, "*US aims to ban Chinese technology in undersea telecommunications cables*," (July 16, 2025), Reuters, https://www.reuters.com/world/china/us-aims-ban-chinese-technology-submarine-cables-ft-reports-2025-07-16/; *see also* Demetri Sevastopulo, "*US set to ban Chinese technology in submarine cables*," (July 16, 2025), Financial Times, https://www.ft.com/content/8ac34fb9-6a51-4343-bfe4-fea566b4fa8c.
[8] *Id* at 7.

2. For each cable system identified in response to Question 1, list all entities that have been contracted, subcontracted, or otherwise authorized to perform construction, repair, or maintenance services since January 1, 2018.
    a. Specifically identify any entity with known or reasonably suspected direct or indirect ties, financial, operational, or beneficial, to the government of the PRC or the Russian Federation. This includes, but is not limited to, SBSS, China Telecom, China Unicom, Huawei Marine, or their affiliates, successors, or shell entities.

3. Please describe in detail the technical, operational, and procedural safeguards employed by your company to protect subsea cable segments during repair, maintenance, or upgrade activities, particularly when performed in international waters or by foreign-flagged or foreign-crewed vessels.
    a. Include all applicable technical or procedural controls such as encryption standards, tamper-evident mechanisms, audit trails, remote logging, multi-party verification, and physical security measures during handling of subsea cable components.

4. Has your company **EVER** identified, detected, or been made aware of any instance of actual or suspected hardware tampering, optical signal tapping, unexpected signal distortion, unauthorized physical access, anomalous latency, unexplained data rerouting, or other operational irregularity during or following any cable repair or maintenance event involving a system in which your company has a material interest?
    a. If yes, please provide the date(s), affected system(s), nature of the incident(s), method(s) of detection, and any remedial or investigative actions taken in response.

5. What specific protocols or procedures does your company have in place for monitoring, reporting, and responding to the presence of foreign-flagged or foreign-operated vessels, particularly those with known or suspected ties to the PRC or the Russian Federation, within proximity to subsea cables, cable routes, or landing stations relied upon by your company?
    a. Please describe any escalation protocols, coordination with U.S. government authorities, or internal monitoring tools used to track such proximity events.

6. Does your company require any foreign or domestic vendors, partners, landing station operators, or maintenance contractors with physical access to subsea cable systems to undergo national security vetting, foreign ownership, control, or disclosure screening, or geopolitical risk evaluation prior to being granted access to cable systems relied upon by your company?
    a. If yes, please provide the applicable contractual language, governance policies, or risk-evaluation frameworks used to enforce these requirements.

7. Has your company **EVER** received, or participated in, any threat briefing, related to foreign adversarial activities targeting subsea cables, including threats posed by entities affiliated with the PRC or Russian Federation, delivered by the U.S. government or an industry coordination body? This includes, but is not limited to, any engagement with or information provided by the National Security Council, Department of Homeland Security, Department of Defense, National Security Agency, Federal Bureau of Investigation, or any Information Sharing and Analysis Center (ISAC) or industry forum.
    a. If yes, please identify the agency or entity involved, the date(s) of the engagement or communication, and a summary of the issues discussed, including any specific risks, threat actors, or recommended mitigation measures.

Additionally, we request that each of your companies coordinate with Committee staff to provide a briefing to the Homeland Security, China Select, and Foreign Affairs Committees no later than August 8, 2025.

Please contact Homeland Security Committee Majority staff at (202) 226-8417, China Select Committee Majority staff at (202) 226-9678, or Foreign Affairs Committee Majority staff at (202) 226-8467 with any questions about this request.

Under Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

House Resolution 5 delegates to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party broad authority to investigate and submit policy recommendations on countering the Chinese Communist Party's economic, technological, security, and ideological threats to the United States and allies and partners of the United States.

Under House Rule X, the Committee on Foreign Affairs has legislative and oversight jurisdiction over "[r]elations of the United States with foreign nations generally" and "measures to foster commercial cooperation with foreign nations and to safeguard American business interests abroad."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,

CARLOS A. GIMENEZ
Chairman
Subcommittee on Transportation
and Maritime Security
Committee on Homeland Security

JOHN MOOLENAAR
Chairman
Select Committee on the CCP

KEITH SELF
Chairman
Subcommittee on Europe
Committee on Foreign Affairs

Encl.

cc: The Honorable LaMonica McIver, Ranking Member
Subcommittee on Transportation and Maritime Security

The Honorable Raja Krishnamoorthi, Ranking Member
Select Committee on the CCP

The Honorable William Keating, Ranking Member
Subcommittee on Europe