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

In the Matter of	)	
	)	
Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks	)	OI Docket No. 24-523
	)	
Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules	)	MD Docket No. 24-524

COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION ("TIA")

I. INTRODUCTION

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input regarding the Federal Communications Commission's ("FCC" or "the Commission") Notice of Proposed Rulemaking ("NPRM") reviewing submarine cable landing license rules and procedures.[1] TIA represents over 400 manufacturers and suppliers of telecommunications equipment and services. TIA members design, produce, market, and manage the information communications technology ("ICT") equipment and services that connect Americans to high-speed broadband networks. Our members include major vendors of

[1] *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, et al.*, Notice of Proposed Rulemaking, FCC 24-119 (2024) ("NPRM").

equipment that comprise subsea cable networks, and it is primarily from this perspective – not of parties directly applying for licenses to operate cables – that TIA files our comments.

TIA shares the Commission's goal of securing the nation's communications infrastructure and applauds the FCC for taking steps to reform the submarine cable rules to further protect national security. TIA offers the following recommendations in furtherance of that goal:

(1) **The FCC should use this opportunity to further enhance supply chain security by applying brightline rules to exclude untrusted vendors from submarine cable networks.** Current targeting and restrictions on untrusted vendors in the licensing process are vague and ad-hoc. The FCC should rely on rules and exclusion lists to improve market certainty and ensure a comprehensive, harmonized approach that supports U.S. national security.

(2) **The FCC can leverage industry standards to help secure submarine cable supply chains.** Harmonized and flexible standards are essential for subsea cable operators to protect cable infrastructure in a dynamic threat environment. In addition to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"), standards like TIA's Supply Chain Security Management System ("SCS 9001")[2] can increase transparency and ensure that supply chains are secure.

(3) **The FCC should seek to streamline the application process and provide certainty to applicants.** This supports U.S. national security by ensuring that there is redundant capacity in the event of a cable cut or other incident involving subsea cables. It also supports the industrial capacity of trusted vendors, as well as a broader ecosystem of high-value goods and services.

By taking these steps, TIA believes that the Commission can both increase security and ease burdens for applicants, helping the U.S. maintain its position as the global leader in vital emerging industries such as artificial intelligence that rely on a robust global telecommunications infrastructure.

[2] *Supply Chain Security*, Telecommunications Industry Association, https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/ (last visited Apr. 10, 2025).

II. THE FCC SHOULD USE THIS OPPORTUNITY TO FURTHER ENHANCE SUPPLY CHAIN SECURITY BY APPLYING BRIGHTLINE RULES TO EXCLUDE UNTRUSTED VENDORS

TIA has been vocal about the threats posed by untrusted vendors to U.S. telecommunications networks, and we have consistently supported FCC action to require that U.S. telecommunications network operators and other customers do not use covered software and hardware from sources that pose national security risks.[3] The security risks posed by untrusted vendors do not stop at the water's edge. Untrusted vendors like Huawei, ZTE, and others in the subsea cable supply chain could help U.S. adversaries to intercept or otherwise interrupt data flowing between countries. At the supplier level, this could be achieved by an untrusted cable vendor, for example, that might be susceptible to a fiber optic tap[4] or by selling products that contain small imperfections that make it susceptible to external stimuli such as radiation[5] or by the creation of a "fiber fuse" effect.[6] Similarly, untrusted electronics have been found to be a vector for supply chain hacks by U.S. adversaries.[7]

With these potential risks in mind, limiting participation by untrusted vendors is a reasonable requirement that promotes U.S. national security. While starting with Covered List vendors makes sense, the FCC should also collaborate with its national security counterparts in the federal government to investigate the need for additional restrictions to cover the range of threats that specifically impact subsea cables. In the subsea cable context, there are other high-risk companies who are active participants in the subsea cable supplier ecosystem. These

[3] See Comments and Reply Comments of the Telecommunications Industry Association, WC Docket No. 18-89
[4] Ciena, In the Lab: Hacking an Optical Fiber Line in Minutes, Ciena (May 18, 2022), https://www.ciena.com/insights/videos/In-the-Lab-Hacking-an-Optical-Fiber-Line-in-Minutes.html.
[5] E. Joseph Friebele, Charles G. Askins, and Michael E. Gingerich, *Effect of low dose rate irradiation on doped silica core optical fibers*, Applied Optics 23, (1984)
[6] Raman Kashyap, *The Fiber Fuse—From a Curious Effect to a Critical Issue: A 25th Year Retrospective*, 21 Optics Express 6422 (2013), https://opg.optica.org/oe/fulltext.cfm?uri=oe-21-5-6422&id=250632.
[7] Jordan Robertson & Michael Riley, *The Long Hack: How China Exploited a U.S. Tech Supplier*, Bloomberg (Feb. 12, 2021), https://www.bloomberg.com/features/2021-supermicro/.

companies have also all been added by the Department of Commerce Bureau of Industry and Security ("BIS") to its Entity List either because they were "acquiring and attempting to acquire U.S.-origin items in support of military modernization for the People's Liberation Army"[8] or because they were "implicated in human rights violations and abuses" against the Uighurs and other ethnic groups in China's Xinjiang region.[9] The involvement by these entities with China's military and state-led efforts to oppress and surveil ethnic minorities raises concerns about the relationships between these companies and the country's security services. Even if these entities were not close to the government, Article 7 of China's National Intelligence Law[10] as well as Article 28 of China's Cybersecurity Law require companies to partner with and share an unlimited amount of data with the China's Ministry of State Security, Ministry of Public Security, and other state intelligence services.[11]

Applying brightline rules and restrictions to these entities, reflective of the Covered List process and in coordination with national security partners, would allow subsea cable owners and operators to more readily respond to ecosystem threats. By identifying and restricting additional countries, entities, technologies, and transactions of concern, the Commission and its partners would also improve industry's ability to zero in on the most advanced threats. Publication of prohibitions and restrictions on specified transactions alongside the development of standard

---

[8] Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List, 86 Fed. Reg. 71557, 71558 (Dec. 17, 2021), https://www.federalregister.gov/documents/2021/12/17/2021-27406/addition-of-certain-entities-to-the-entity-list-and-revision-of-an-entry-on-the-entity-list. Relevant entities listed here include: HMN Technologies (formerly a part of Huawei) , HMN parent company Jiangsu Hengtong Group, and Zhongtian Technology Submarine Cable.

[9] Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List, 85 FR 34503, 34504 (June 5, 2020), https://www.federalregister.gov/documents/2020/06/05/2020-10868/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entries-on-the-entity-list.

[10] 全国人民代表大会常务委员会, 中华人民共和国国家情报法, April 27, 2018 https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4NDk4ZDA5ZjE%3D.

[11] 新华社，中华人民共和国网络安全法，June 29, 2018, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

mitigation practices for certain classes of risks would clarify and crystallize the restrictions required to protect national security.

While we believe that applying brightline rules and restrictions to protect subsea cable infrastructure from cybersecurity and supply chain threats is critical, we acknowledge that doing so for projects that are already substantially underway or that are already completed would create significant challenges. Requiring licensees to remove or "rip and replace" such equipment or services in a manner consistent with the Secure Networks Act, as suggested by the Commission, would lead to substantial cost constraints.[12] Given that the Secure Networks Act funding has yet to be fully dispersed as well as the practical limitations of addressing infrastructure which both crosses national boundaries and in some cases is sitting underwater, the costs of an undersea "rip and replace" type program would likely outweigh the benefits.

III. SUPPORT FOR CYBER AND SUPPLY CHAIN STANDARDS CAN DRIVE SECURITY IMPROVEMENTS

In the NPRM, the Commission proposes requiring applicants and reporting licensees to certify that they have "created, updated, and implemented cybersecurity risk management plans," and that they take "reasonable measures to protect the confidentiality, integrity, and availability of their systems and services that could affect their provision of communications services."[13]

[12] NPRM, para. 100.

[13] *Id*. ¶ 108, Proposed Rule § 1.7006(c). While acknowledging that "there are many ways that applicants or licensees may satisfy the [cybersecurity risk management plan] requirement," the Commission proposes that an applicant or licensee "could . . . demonstrate compliance with this proposed requirement by following an established risk management framework, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)." The Commission also proposes that an organization's cybersecurity risk management plan would have to describe its "implementation of security controls sufficient to ensure the confidentiality, integrity, and availability of all aspects of their communications systems and services." While acknowledging there are "many ways for applicants and licensees to satisfy this aspect of the requirement," the Commission proposes that "applicants and licensees will satisfy it if they demonstrate they have successfully implemented an established set of cybersecurity best practices, such as the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector

TIA appreciates the FCC referencing the value that the NIST CSF can provide as a basis for these plans, and the potential utility of other standards and risk management frameworks to protect the security of our subsea cable infrastructure.

Other standards, such as TIA's SCS 9001, are specifically relevant here given it is an industry-developed standard that seeks to drive greater supply chain transparency by creating a common benchmark for a range of factors including: hardware and software provenance, counterfeit parts, secure development processes, software usage, and a range of other requirements. SCS 9001 is a certifiable, process-based global standard with a specific focus on securing the supply chain of organizations operating in the ICT industry. SCS 9001 provides assurance of the proper operational hygiene of network operators and their suppliers in delivering products and services of inherently higher security. It also includes specific mechanisms to address concerns regarding supply chain security and transparency, and includes a section requiring transparency around business practices and the extent to which vendors can operate independently of governments in the jurisdiction in which they are headquartered. SCS 9001 also specifically excludes companies on the basis of government national security risks.[14] SCS 9001 would provide the FCC with a common rubric for analyzing a range of risks by participants in the subsea cable supply chain and would help companies deploying subsea cables understand risks posed by potential suppliers.

A Commission approach centered around common and well-regarded frameworks and standards, such as the NIST CSF and SCS 9001, would promote uniformity and protect the needs

Cybersecurity Performance Goals (CPGs) or the Center for Internet Security Critical Security Controls (CIS Controls)." *Id*. ¶¶ 110-113.

[14] *TIA Policy on U.S. Government Restrictions (Version 2.0)*, TIA (2025), https://tiaonline.org/wp-content/uploads/2024/01/TIA-Policy-on-Government-Restrictions.pdf.

of industry to remain agile and flexible in a highly dynamic threat environment.[15] The Commission should ensure any cybersecurity, supply chain, and sensitive data requirements that it requires do not conflict with other agency directives. Harmonized cybersecurity requirements based in common standards and frameworks can reduce the costs of compliance, allowing subsea cable licensees to direct resources toward improving threat detection and response.

In sum, the Commission should ensure applicants and licensees have the flexibility to rely on trusted frameworks and standards, such as the CSF and SCS 9001, as part of a comprehensive cybersecurity plan to respond to rapidly evolving cyber and supply chain threats.[16] The Commission should avoid imposing cybersecurity requirements that may conflict with other requirements with which communications providers may have to comply. It should coordinate with its national security counterparts in other federal agencies to harmonize subsea cable cybersecurity requirements and supply chain restrictions and allow operators to rely on certified cybersecurity plans informed by the NIST CSF, the FCC Covered List, and SCS 9001.[17] Allowing subsea cable licensees to leverage the CSF and standards such as SCS 9001 will permit operators to implement tailored security controls and dynamically adapt to evolving cyber threats.

IV. STREAMLINED AND EFFICIENT PROCESSES SUPPORT ECONOMIC AND NATIONAL SECURITY

The FCC should work in coordination with other executive branch agencies to develop

[15] *See* Delete, Delete, Delete Public Notice available at DA-25-219A1.pdf.
[16] NPRM ¶ 110.
[17] *The NIST Cybersecurity Framework (CSF) 2.0*, NIST (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, FCC, https://www.fcc.gov/supplychain/coveredlist (last updated Sept. 3, 2024).

streamlined processes for trusted applicants that use trusted vendors for subsea cable equipment. A faster regulatory review process for such subsea cable operators would increase investment in the deployment and operation of subsea cables that connect to the United States.

This increased investment would support improving the redundancy of subsea cables and build the industrial capacity of trusted vendors. Subsea cable systems face a variety of threats, from disruptions caused by nature to unintentional cuts by fishing trawlers to cuts by foreign adversaries and potentially cyberattacks.[18] A system with redundant cables is thus essential; when a cable is cut or otherwise disrupted, operators can route data traffic through other cables without substantial disruption to communications.[19]

Increased investment in trusted equipment for subsea cables also improves the industrial capacity of trusted vendors and supports a broader ecosystem of digital services. Companies based in foreign adversary nations have significant market share in the manufacturing and installing of subsea cables.[20] And various other communications companies based in foreign adversary nations—such as ZTE—provide equipment for subsea cables.[21] To compete, the United States should help support trusted vendors.

Increased investment in a robust subsea cable system also would support the digital services and economic sectors that rely on them for communications services. Subsea cable

---

[18] Daniel F. Runde et al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS (Aug. 16, 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition; Justin Sherman, *Cyber defense across the ocean floor: The geopolitics of submarine cable security*, Atlantic Council (Sept. 13, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

[19] Daniel F. Runde et al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS (Aug. 16, 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

[20] Daniel F. Runde et al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS (Aug. 16, 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

[21] *See, e.g.*, Press Release, *ZTE collaborates with Link Net's First Media to boost network services for information superhighway in Jayabaya Project*, ZTE (April 26, 2022), https://www.zte.com.cn/global/about/news/20220426e1.html.

systems are estimated to carry 99 percent of intercontinental traffic, supporting businesses and government communications that utilize global traffic flows.[22] As the Department of Homeland Security has explained, without subsea cables "our smartphones, financial networks, and communications systems would cease to function reliably . . . [and] its continuous, secure, and resilient operation [is] a critical requirement for U.S. national and economic security."[23]

To support trusted vendors and investment in secure subsea cable equipment, the FCC and Team Telecom agencies should implement a fast-track process for trusted subsea cable licensees and applicants. The United States already is one of the more challenging places to land subsea cables due to a fragmented regulatory landscape and drawn out review process.[24] Yet trusted partners and subsea cable systems that don't present specific national security concerns must undergo the same rigorous review process that untrusted entities and systems that raise particular national security risks must undergo. Trusted licensees and applications should include entities that already have subsea cable licenses, otherwise have undergone rigorous Team Telecom national security reviews, or whose applications do not present exceptional national security risks. A streamlined review process would reduce the administrative burden, and burden on subsea cable operators and investors.

This process should apply to licensees and applicants that commit to using trusted equipment vendors. As discussed above, the use of equipment from untrusted vendors may present significant national security concerns, including the risk of surveillance by foreign adversaries or disruptions to data flows through subsea cables. On the other hand, trusted

---

[22] Department of Homeland Security, *Priorities for DHS Engagement on Subsea Cable Security & Resilience*, 1 (December 2024), https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.

[23] *Id.*

[24] Department of Homeland Security, *Priorities for DHS Engagement on Subsea Cable Security & Resilience*, 5 (December 2024), https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.

equipment vendors may not present the same national security concerns. Subsea cable operators that use trusted equipment should not have to undergo the same review process as those that use untrusted equipment. As discussed above, by utilizing standards such as SCS 9001, providers will have the ability to monitor and take action on their supply chain risks providing even more assurance that a streamlined process would be appropriate.

Additionally, the FCC should not undertake any actions that would increase the risk of investment in subsea cables or undermine existing investments. Accordingly, the FCC should maintain the existing 25-year license term for subsea cable licenses.[25] Subsea cable systems require substantial upfront investment—often running hundreds of millions of dollars—and often require coordination among a consortium of investing businesses.[26] Shortening these license terms would unnecessarily insert additional risk, thereby undermining investment in subsea cables. If the FCC moves forward with the proposed subsea cable regulations, it should not impose new requirements on licensees before the original license term expires.[27]

By streamlining the review process for trusted subsea cable licensees and applicants using trusted equipment vendors, the FCC would support investment in subsea cables without undermining national security. The Commission should not move forward with the rules proposed in the NPRM that would place even more burdens on licensees, applicants, and administrative agencies without corresponding national security benefits, lest it place even more regulatory hurdles in the way of investment in this critical infrastructure.

[25] 47 CFR § 1.767(g)(15). *But see* NPRM ¶ 59.
[26] Department of Homeland Security, *Priorities for DHS Engagement on Subsea Cable Security & Resilience*, 4 (December 2024), https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.
[27] *But see* NPRM ¶¶ 68-71 (discussing retroactivity concerns with shortening license terms and applying new regulations or denying renewal applications before original license terms expire).

V. CONCLUSION

TIA appreciates the FCC's attention to the importance of the security of the global subsea cable infrastructure. We believe this docket is an excellent opportunity for the FCC to both streamline the overall licensing process and enhance national and economic security by addressing issues related to untrusted vendors. We thank the FCC for the opportunity to provide comment, and we look forward to additional opportunities to support the Commission's work in this area.

Patrick Lozada
Director, Global Policy

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard
Floor 27
Arlington, VA 22204
(703) 907-7733

Filed: April 14, 2025