Federal Communications Commission

Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks

47 CFR Parts 0 and 1
[OI Docket No. 24-523, MD Docket No. 24-524; FCC 26-42, FR ID 357134]

AUTHORS

Craig Singleton
Senior Director and Senior Fellow, FDD's China Program

RADM (Ret.) Mark Montgomery
Senior Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Jack Burnham
Senior Research Analyst, FDD's China Program

Washington, DC
August 19, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Beijing's efforts to dominate, and establish the conditions to disrupt, U.S. and global submarine cable infrastructure pose a direct threat to American national security. These cables carry nearly 95 percent of global internet traffic, including commercial transactions, government services, and civilian communications.[1]

In response, the Federal Communications Commission (FCC) has tightened scrutiny over the sector. This includes expanding licensing requirements for owner-operators, prohibiting the use of components produced by Covered List firms, and heightening cybersecurity and physical security requirements around sensitive locations. Collectively, these actions have strengthened protections against a range of threat vectors while streamlining the administrative burden for owner-operators to expand their buildout of critical infrastructure essential for the American economy.

However, several regulatory gaps remain, posing a national security risk. While the FCC has tightened scrutiny over some cable owner-operators, the commission should tighten routine conditions for cable landing licenses used by submarine line terminal equipment (SLTE) owner-operators, which face unique threats given the relative vulnerability of landing stations and other related assets.

The commission itself has described SLTE as "among the most important equipment associated with the submarine cable system." SLTE sits at the point where undersea capacity is terminated, managed, and connected to terrestrial networks, making control over the equipment, its software, and its remote-management functions particularly consequential for the confidentiality, integrity, and availability of cable traffic.[2]

Current Regulatory Gaps May Contribute to Security Vulnerabilities

In October 2025, the commission reaffirmed that any entity owning or controlling a 5 percent stake in a cable network and using the U.S. points of the system must apply for a license. In July

[1] RADM (Ret.) Mark Montgomery, Craig Singleton, Jack Burnham, and Annie Fixler, "Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Schedule of Application Fees," *Foundation for Defense of Democracies*, April 14, 2025. (https://www.fdd.org/analysis/2025/04/14/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security-law-enforcement-foreign-policy-and-trade-policy-risks-schedule-of-application-fees)

[2] U.S. Federal Communications Commission, Office of International Affairs, Second Report and Order and Second Further Notice of Proposed Rulemaking, "Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks," June 30, 2026. (https://docs.fcc.gov/public/attachments/FCC-26-42A1.pdf)

2026, this mandate was partially expanded to current and future SLTE owner-operators.[3] These measures, combined with both annual and one-time reporting requirements and new security mandates, allows the commission to map vulnerabilities within U.S. submarine cable infrastructure while proactively denying access to foreign adversaries incapable of clearing a national security review.[4] The expansion of the commission's licensing regime also expands its capacity to enforce critical security standards, including preventing owner-operators from using components produced by Covered List entities and requiring more stringent cyber and physical security measures.[5]

However, several key gaps remain within the FCC's efforts to further secure submarine cable infrastructure. Although the commission launched a one-time data collection effort to capture potential vulnerabilities across domestic SLTE infrastructure, there is currently no regulatory requirement for SLTE owner-operators to provide updated filings to the FCC as a condition of maintaining their license.[6] Moreover, the blanket license offered to these entities ensures that other additional users operating on their infrastructure are not inherently subject to rigorous national security standards, producing both a visibility and enforcement gap.[7]

The dangers of these gaps are clear. In contrast to the cables themselves, which are often deep underwater, landing stations are more easily accessible, often appearing in remote locations that lack strong physical security measures.[8] Moreover, their remoteness contributes to a high rate of

---

[3] Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, U.S. Federal Communications Commission, 90 Federal Register 48648, October 27, 2025. (https://www.federalregister.gov/documents/2025/10/27/2025-19658/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security); Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Second Report and Order, U.S. Federal Communications Commission, 91 Federal Register 46844, July 27, 2026. (https://www.federalregister.gov/documents/2026/07/27/2026-15123/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security)

[4] Information Collection Being Reviewed by the Federal Communications Commission, U.S. Federal Communications Commission, 91 Federal Register 50834, August 6, 2026. (https://www.federalregister.gov/documents/2026/08/06/2026-15932/information-collection-being-reviewed-by-the-federal-communications-commission)

[5] U.S. Federal Communications Commission, Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, "Report and Order and Further Notice of Proposed Rulemaking," August 13, 2025. (https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf)

[6] Information Collection Being Reviewed by the Federal Communications Commission, U.S. Federal Communications Commission, 91 Federal Register 50834, August 6, 2026. (https://www.federalregister.gov/documents/2026/08/06/2026-15932/information-collection-being-reviewed-by-the-federal-communications-commission)

[7] Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Second Report and Order, U.S. Federal Communications Commission, 91 Federal Register 46844, July 27, 2026. (https://www.federalregister.gov/documents/2026/07/27/2026-15123/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security)

[8] Jack Burnham, RADM (Ret.) Mark Montgomery, and Craig Singleton, "Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks," *Foundation for Defense of Democracies*, November 20, 2025.

remotely controllable components and third-party access arrangements, increasing the possibility of damaging cyberattacks or state-sponsored espionage campaigns.[9]

These risks extend beyond formal ownership. SLTE and related cable infrastructure may depend on third parties for network management, software and firmware updates, diagnostics, hosting, repair, and maintenance. A trusted cable owner can therefore remain exposed if an untrusted vendor, subcontractor, network operations center, or maintenance provider retains privileged cyber, or physical, access to critical systems. The commission should ensure that its rules capture who can access, maintain, modify, update, or remotely administer SLTE, rather than relying principally on ownership of the equipment itself.

Recent PRC cyber activity illustrates the stakes. In its 2025 submarine-cable rulemaking, the FCC cited U.S. government findings that PRC state-sponsored actors associated with the Salt Typhoon campaign penetrated at least eight U.S. communications companies.[10] The episode demonstrates why communications infrastructure must be secured against persistent access through management systems, service providers, and other trusted relationships in addition to the hardware itself.

Recommendations

The FCC should build on its previous efforts to strengthen scrutiny over submarine cables by tightening routine conditions for cable landing licensees. These efforts should focus on ensuring that SLTE owner-operators, which face heightened cyber and physical security threats due to the accessibility of their assets, maintain strong security protocols with terms that are reviewable by other executive branch agencies and are enforceable via contractual obligations.

- **The FCC should require these licensees to ensure that any entity that owns and/or operates SLTE on their licensed submarine cables adheres to stringent national security standards.** This proposal produces a necessary layer of oversight for sub-contractors and other users or lessees that rely on SLTE by adding a separate contractual enforcement mechanism for the commission's previously articulated national security regulations outlined in its First and Second Report and Order. Moreover, this model will reduce the administrative burden of complying with new routine conditions by ensuring that national security concerns rest within preexisting commercial contracting processes.

(https://www.fdd.org/analysis/2025/11/20/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security-law-enforcement-foreign-policy-and-trade-policy-risks)

[9] Ibid.

[10] U.S. Federal Communications Commission, Second Report and Order and Second Further Notice of Proposed Rulemaking, "Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks," June 30, 2026. (https://docs.fcc.gov/public/attachments/FCC-26-42A1.pdf)

These contractual requirements should expressly flow down to downstream operators, maintenance and repair providers, network operations centers, software and firmware providers, and other entities with physical or logical access to SLTE. Licensees should be required to maintain sufficient information to identify who owns, operates, services, remotely accesses, or can modify the equipment and to ensure that changes to those relationships do not create a foreign-adversary access pathway. This approach would build directly on the commission's existing restrictions on foreign-adversary-controlled third-party service providers.

- **The FCC should require consistent, routine conditions for licensees, regardless of whether they own and/or operate SLTE on their licensed submarine cable; own an SLTE and either own or lease the underlying fiber, capacity, or spectrum; or lease the SLTE and the underlying fiber, capacity, or spectrum to another entity.** The commission should ensure that licensees, regardless of their business model, must comply with the same security standards to reduce the risk of vulnerabilities due to differing regulatory standards. National-security requirements should follow access and operational capability rather than corporate form. An entity capable of configuring SLTE, accessing network-management systems, changing firmware, controlling a network operations center, or otherwise affecting cable operations can create comparable risk whether it owns the underlying fiber or participates through a lease, service agreement, or subcontract.

- **The FCC should require that cable landing licensees implement and regularly update enhanced cybersecurity and physical security plans in accordance with best practices.** As submarine cables remain a key facet of U.S. critical infrastructure and underpin military mobility, the commission should ensure that their owner-operators comply with the highest standards of physical and cybersecurity. Licensees should be required to comply not only with guidance offered by the National Institute of Standards and Technology's cybersecurity framework, but also with either the Cybersecurity and Infrastructure Security Agency's Cybersecurity Performance Goals, or the Center for Internet Security's Critical Security Controls. Moreover, licensees should also be periodically required to assert their compliance with the commission, institutionalizing previously ad-hoc data-collection efforts to garner greater insight into the sector.

- **The FCC should extend its incident-reporting standard to all cable landing licensees and SLTE owners and operators.** The Second Report and Order requires applicants qualifying for streamlined executive branch review to report, within 72 hours, information reasonably indicating unauthorized access to, disruption of, or corruption of a submarine cable system, including incidents affecting SLTE operators and third-party

service providers. The commission should make this a routine baseline condition across the SLTE ecosystem. Reportable events should include unauthorized physical or cyber access, compromise of network-management information, unauthorized system modifications, significant attempted intrusions, and other incidents capable of affecting the confidentiality, integrity, or availability of the cable system. A common reporting obligation would give the FCC and its federal partners faster visibility into threats that can move across multiple owners, operators, and service providers.

- **The FCC should require heightened access controls for personnel and contractors with privileged SLTE access.** At a minimum, licensees should maintain auditable records identifying individuals and third parties with physical or cyber administrative access; apply least-privilege and multifactor-authentication requirements; promptly terminate credentials when access is no longer required; and impose heightened scrutiny on remote access originating from foreign-adversary jurisdictions. These safeguards are especially important where equipment can be remotely configured or maintained without personnel entering a landing station.

- **The FCC should require applicants with reportable foreign ownership that seek exemption from referral to an Executive Branch agency to submit responses to the Standard Questions directly to Team Telecom.** The commission has continuously strengthened its capacity to scrutinize applications over the past two rulemaking cycles, an effort that it should continue to avoid producing inadvertent enforcement gaps. To this point, the Standard Questions provide critical information to ensure the quality of the committee's national security determinations, including details that are not included within the national security standards adopted by the Second Report and Order. As such, this information should be collected across both processes to inform the FCC's regulatory actions.

- **The FCC should use this proceeding to reinforce a trusted-supplier model across the submarine-cable lifecycle.** Security assessments should account for the provenance of SLTE hardware, software, firmware, network-management platforms, maintenance services, and other components capable of accessing or altering cable operations. This approach is consistent with the United States and allied governments' broader commitment to secure and verifiable subsea-cable providers, transparent ownership and governance, and recurring security-risk assessments across the cable lifecycle. The United States and partners endorsed those principles in their 2024 Joint Statement on the Security and Resilience of Undersea Cables.[11]

[11] U.S. Department of State, Press Statement, "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," September 26, 2024. (https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world)

Conclusion

Beijing's efforts to dominate access to, and establish the conditions to potentially disrupt, U.S. and global submarine cable infrastructure pose a direct threat to American national security. The FCC should strengthen its mandated routine conditions for cable landing licenses to safeguard SLTE infrastructure from cyberattacks and physical sabotage, to protect the United States from foreign-adversary risk entering through downstream operators, remote-access relationships, maintenance providers, or other third parties. Consistent baseline cybersecurity, access-control, incident-reporting, and supply-chain requirements would close the remaining gaps while preserving the commission's streamlined licensing framework for trusted operators.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the final rule.