Priorities for DHS Engagement on Subsea Cable Security & Resilience

A White Paper by the Office of Economic Security, the Supply Chain Resilience Center, and the Cybersecurity and Infrastructure Security Agency

Overview

The U.S. Department of Homeland Security (DHS) is a leader in the U.S. government's cybersecurity and critical infrastructure security and resilience efforts. As such, DHS, through the Office of Strategy, Policy, and Plans (PLCY) and the Cybersecurity and Infrastructure Security Agency (CISA), convened a group of representatives from the Departments of Defense, Justice, Commerce, Treasury, State, the Federal Communications Commission, and the Intelligence Community to hold a series of engagements with industry stakeholders in the subsea telecommunications cable sector. The purpose of these engagements was for departments and agencies across the U.S. government to gather perspectives from leading cable manufacturers, owners, operators, and equipment vendors on challenges to subsea cable network security and resilience and to identify opportunities to mitigate these issues. These engagements also allowed U.S. government representatives to share policy priorities and opportunities to further strengthen the resilience and security of subsea cable systems.

This paper outlines key findings from these industry engagements and identifies three areas where DHS will focus its near-term efforts to improve coordination on cable issues.

DHS, through similar interagency engagements and its statutory authorities that convene critical infrastructure owners and operators, will continue to engage the subsea cable industry to strengthen the security and resilience of these systems. DHS values its relationships with industry stakeholders to ensure mutual understanding of the challenges and opportunities facing the cable industry and U.S. national security.

About the Office of Economic Security and the Supply Chain Resilience Center

PLCY's Office of Economic Security aims to safeguard U.S. national and economic security against foreign threats using an array of tools, including foreign investment screening, risk mitigation, and cross-cutting policy initiatives.

The DHS Supply Chain Resilience Center (SCRC) leverages DHS programs and authorities to enhance the resilience of supply chains which are crucial for homeland security. It serves as a hub where industry and government come together to address supply chains that support the economy and the functioning of critical infrastructure. The SCRC relies on integrated supply chain analysis to anticipate, monitor, and respond to supply chain risks and identify approaches to mitigate risks that enhance availability and integrity of critical supplies and health of related supply chains.

About CISA

As the nation's cyber defense agency and national coordinator for critical infrastructure security, the Cybersecurity and Infrastructure Security Agency leads the national effort to understand, manage, and reduce risk to the digital and physical infrastructure Americans rely on every hour of every day.

Acknowledgement

DHS extends its sincere appreciation to the interagency partners as well as the cable owners, operators, vendors, suppliers, and service providers who made the effort to participate in these engagements, often on-site in Washington, DC. On behalf of interagency partners from across the federal government, we thank all industry representatives for the candid and highly informative discussions. While many of the insights and concerns shared during these engagements are not directly referenced in this white paper, DHS and the interagency look forward to collaborating further to ensure that all such issues are incorporated into future engagements and projects outlined herein.

INTRODUCTION

The vast underwater network of subsea telecommunications cables is one of the most critical systems of infrastructure in our world today, estimated to carry around 99 percent of intercontinental data traffic[1] without which our smartphones, financial networks, and communications systems would cease to function reliably. This network's increasingly vital role in global communications and economic growth makes its continuous, secure, and resilient operation a critical requirement for U.S. national and economic security.

At the same time, public threats to this network from foreign adversaries have raised concerns over the potential impact of intentional disruption of subsea cables, which are already exposed to significant risk of disruption from an array of man-made and natural threats.[2] Despite an overarching need to enhance the security and resilience of this critical infrastructure, doing so is difficult due to cable systems' diversified international ownership, their multinational connections, and their presence in the global commons. Consequently, successfully expanding, maintaining, and protecting this network will depend on increased partnership between government and industry to develop solutions to shared problems.

It is the policy of the United States that a continuous national effort—coordinated between government and industry—is needed to secure critical infrastructure, including subsea cables.[3] As with most critical infrastructure assets, subsea cable systems are generally privately owned and operated, but as the backbone infrastructure of the global internet and telecommunications network, the loss or unavailability of these cables poses risks to the public, including to the national and economic security of the United States.[4]

DHS plays a key role in the U.S. government's approach to securing subsea telecommunication cables and associated systems and recognizes the importance of maintaining U.S. leadership in the sector. Therefore, the Office of Economic Security, the Supply Chain Resilience Center (SCRC), and the Cybersecurity and Infrastructure

Security Agency (CISA) co-hosted a series of engagements between multiple Federal departments and leading owners, operators, equipment vendors, and suppliers in the subsea cable industry. These engagements sought to:

1. Improve the U.S. government's understanding of threats to and vulnerabilities of the subsea cable ecosystem from a variety of industry perspectives;
2. Share and discuss the U.S. government's policy priorities for cable infrastructure; and
3. Identify opportunities to cooperatively strengthen the security and resilience of subsea cable systems.

While industry representatives provided many insights into the dynamics of the subsea cable market, this paper outlines a few key takeaways and common themes that highlight opportunities for DHS and its federal partners to improve coordination and collaboration with the private sector; streamline permitting, licensing, and regulatory processes; and clarify federal roles and responsibilities for cable emergency management and incident response.

DHS'S ROLE IN CABLE SECURITY AND RESILIENCE

DHS, through CISA, is the U.S. government's National Coordinator for Critical Infrastructure Security and Resilience, applying its statutory authorities to address systemic and cross-sector risk by working across the federal government and industry to identify, analyze, prioritize, and manage the most significant risks to critical infrastructure.[5] Under the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), CISA also serves as the President's designated Sector Risk Management Agency for the Communications and Information Technology sectors—each of which play a crucial role in the subsea cable ecosystem.[6]

The United States Coast Guard and U.S. Customs and Border Protection leverage their maritime presence and law enforcement authorities to detect, deter, and respond to unusual activity or potential threats against critical infrastructure in the maritime environment, including subsea cables. In accordance with applicable laws and regulations, these DHS components monitor and enforce compliance of vessels operating in U.S. waters, including those laying and repairing cables, as part of their respective missions to safeguard the nation's maritime environment and to facilitate lawful trade and travel.

Additionally, DHS, through its role in the Team Telecom[7] process, secures U.S. subsea cable infrastructure by reviewing foreign ownership and participation in these systems to identify and mitigate national security risks. Team Telecom conducts rigorous evaluations of certain Federal Communications Commissions (FCC) license applications to land subsea cables in the United States, imposes security mitigation agreements, and monitors compliance therewith to protect these critical systems from malign foreign influence. DHS also operates the SCRC, which seeks to leverage DHS programs and authorities to enhance the resilience of supply chains crucial for homeland security, including those that support critical infrastructure.

Finally, DHS and its operational components leverage their vast regional presence across the United States to coordinate closely with the state, local, territorial, and tribal (SLTT) authorities on all matters relating to the protection of critical assets in their respective regions.

DHS POLICY PRIORITIES FOR SUBSEA CABLES

- Ensure continued U.S. leadership in the subsea cable industry.
- Promote secure and resilient subsea cable networks and supply chains and counter foreign adversary threats.
- Enhance public/private partnership.
- Ensure coordinated federal permitting and regulation.
- Promote the development of reliable subsea cable repair capacity.
- Coordinate internationally to increase network resilience and route diversity.
- Support responsible innovation in cable technologies.

SUBSEA CABLE INDUSTRY CONTEXT AND STRESSORS

Threats to Cable Systems

From the first transoceanic cable laid in the late 1850s to the digital transformation of the early 2000s, over half a million miles of subsea cables have been laid globally to serve as the backbone of global telecommunications.[8] This network and its supporting ecosystem are vital to the strategic and economic interests of the United States, but they face complex and challenging risks from natural, accidental, and malicious threats. While two-thirds of cable faults worldwide are attributed to accidental activity like fishing and anchor drags,[9] disruptions to the operation of subsea cables can have immediate and far-reaching effects, given the overwhelming reliance our global communication network has on these systems. The cable industry has long built resilience into its systems to mitigate the effects of the hundreds of incidents that occur every year and predominantly relies on redundancy (multiple systems, excess capacity, and alternate routes) to ensure system-wide resilience while damaged systems undergo repairs. At the same time, however, the resurgence of great power competition increases the potential for foreign adversary interference with subsea communications networks that carry sensitive government and other types of critical information upon which our national and economic security depend.

Regardless of their immediate cause, multiple outages or outages in remote or isolated locations often result in delays, loss of data in-transit, or even internet unavailability. Across our discussions with industry representatives, there was general agreement that the most prolific threats to cable infrastructure are physical threats that present near the shore in shallow water, where the infrastructure is most vulnerable to human activity, such as fishing and commercial shipping. However, it was widely noted that the least likely but most challenging disruption would occur in the deep sea, where damaged cables are harder to access by a cable repair ship. Given ever-increasing capacity demands on cable systems, it is unknown whether current redundancy measures could maintain critical functions in the event of a widespread outage of cables in a relatively confined area.

The geographic concentration of cables, both near land and in deeper waters, exacerbates the risk of widespread damage and disruption. Various technical, geological, financial, and regulatory dynamics tend to lead subsea cables along similar routes in many parts of the world, creating both geographic and geopolitical chokepoints. One such chokepoint, the Red Sea, was the site of a major cable incident when, in February 2024, several subsea fiber-optic cables were damaged by a single ship's anchor dragging along the seabed, which degraded 25 percent of total internet and telecommunications traffic between Europe and Asia.[10] Further, territorial disputes in the South China Sea, through which the vast majority of cables carrying data traffic between Asia are laid, have complicated the free passage of cable laying and repair ships operating in those waters. Requirements to obtain advance permits from the governments claiming those waters has severely hindered the rapid deployment and repair of cables in a critically important pathway for Asia-Pacific data traffic.[11] While incidents in geographic chokepoints are relatively rare, each one brings much-needed attention to the vulnerability of similarly concentrated cables around the world.

Market Dynamics

From a market perspective, the global subsea cable industry is highly concentrated and capital intensive, with high barriers to entry. Today, companies such as Google, Meta, Amazon Web Services, and Microsoft—also known as "hyperscalers"—have replaced traditional telecom providers and common carriers as the primary drivers of global investment in subsea fiber-optic cables, given the growing capacity demands from cloud services, social media, web search, and other streaming services. In 2021, these hyperscalers accounted for 69% of all used international bandwidth.[12] Modern cable systems typically cost hundreds of millions of dollars to construct, with few entities worldwide having the resources and business justification to be the sole investor in a new subsea cable system. Most often, entities wishing to build and operate cable systems form consortia to share the risks and costs associated with such projects.

Together, high barriers to entry and a decreasing pool of investors have concentrated supply chain risks to subsea cable systems. For example, multiple cable industry representatives highlighted the susceptibility of the subsea cable supply chain to shocks, given increased competition from other industries for the same components and materials. On the supplier side, there are only four companies worldwide that provide turnkey subsea cable solutions, from conception, engineering, and manufacturing to construction, installation, and repair. SubCom is the only manufacturer and installer of subsea cables headquartered in the United States. The other three companies are Japan's NEC, China's HMNTech (formerly Huawei Marine Networks), and France's Alcatel Submarine Networks.

The global fleet of ships that lay and repair subsea cables also presents a number of vulnerabilities. Of all the ships capable of laying and repairing subsea cables, there are only 22 such ships in the world dedicated solely to repair, of which only two are U.S.-flagged, and that fleet is aging.[13] While industry has not clearly identified global repair capacity as a current systemic issue, there are significant challenges to securing financing for new ships, given the high capital costs and the long-term nature of such investment. Banks have been reluctant to provide the necessary financing to build new subsea cable ships, and most fleet investment today is dedicated to maintaining and upgrading existing ships to extend their service life. Without timely mitigation, the shrinking of an already limited fleet due to age would present a significant barrier to cable repair capacity. In the event of degraded repair capacity or a widespread, persistent disruption to cable systems, the United States may

have to rely on ships outside of its trusted vendor networks, which could introduce security concerns if the ship operators are subject to the ownership, control, or influence of a foreign adversary.

Regulatory Landscape

In every country where a subsea cable lands, including in the United States, cable owners and operators must obtain a myriad of national, state, and local approvals to lay and operate these systems. These approvals often involve various government bodies charged with ensuring the compliance with environmental, cabotage, commercial, maritime, and national security laws and regulations. Navigating several simultaneous and often conflicting compliance processes across multiple jurisdictions is an increasingly complex and costly aspect of the subsea cable industry.

For most of the subsea cable industry, engagement with the U.S. government typically occurs only within the context of specific permitting, licensing, emergency management, and regulatory discussions regarding individual cable systems. These touchpoints often occur across multiple government agencies with diverse security, economic, or environmental missions. This decentralized approach extends beyond the federal government to state, local, territorial, and tribal authorities that have oversight of subsea cable construction, operation, and maintenance. This means that public-private interactions occur across various siloed processes in a variety of jurisdictions even within the United States.

Regrettably, several industry representatives lamented that governmental authorities' shifting expectations and the increasingly unpredictable outcomes of these processes have made the United States, in their view, one of the most difficult countries in which to land subsea cable systems. This is largely due to the fact that, in the past few years, permitting timelines have, on average, increased from under 12 months to over 3 years' time. This dynamic only amplifies the market-based challenges surrounding investment in these systems, as high uncertainty in project timelines and a high risk of licensing and permitting delays contribute to a declining pool of entities willing to invest in new cable systems.

PRIORITY ACTIONS TO ENHANCE SUBSEA CABLE COORDINATION AND COLLABORATION

DHS's recent cable industry engagements have underscored the criticality of public-private coordination as well as robust and continuous evaluation of government policies and programs that have a direct impact on subsea cable security and resilience. Therefore, DHS will continue to lead industry engagement and will prioritize opportunities to leverage its authorities to encourage continued U.S. leadership of this critical industry. As with all critical infrastructure protection domains, information sharing and cooperative action—across both public and private sectors—are essential to enhancing the United States' collective defense and primacy in critical enabling technologies that confer significant national and economic security advantages. Through these engagements and the federal government's ongoing efforts, DHS has identified three priority areas for improved coordination and collaboration:

1. Enhance Mechanisms for Public-Private Coordination

The interconnected nature of subsea cable systems and the complexity of the industrial ecosystem that builds

and operates them demands close, continuous government-to-industry coordination to anticipate and confront shared security and resilience challenges. These often-systemic challenges ultimately affect everything that relies on international communications, from trillions of dollars of daily financial transactions to sensitive government and military communications. The U.S. government must grow and sustain such coordination to effectively address them.

The subsea cable industry spans multiple critical infrastructure sectors, including communications and information technology, which means that it does not fit cleanly within existing U.S. government mechanisms for engaging critical infrastructure owners and operators, such as Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs).[14] This has limited DHS's and the U.S. government's opportunities to gain insights from the cable industry on its unique risks and challenges. While some entities that own and operate U.S. cable systems are represented within either the Information Technology or the Communications SCCs, those bodies do not include other critical entities within the cable industry that, for example, build, maintain, or equip these systems. In effect, there currently exists no forum in which the full scope of the cable industry can effectively collaborate with the U.S. government to identify and address shared challenges.

Path Forward: DHS will work internally and across the U.S. government to improve subsea cable industry representation and engagement, including by leveraging existing critical infrastructure engagement bodies like SCCs and GCCs, and by exploring new ways to engage industry through forums for ongoing classified and unclassified information exchange. Increased collaboration would also create opportunities to perform joint exercises and better incorporate subsea cable industry-specific insights into the national risk management planning cycle outlined in NSM-22.

DHS has highlighted the challenges associated with cross-sector collaboration as part of its review of the existing Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for federal governmental entities to engage representatives from the community of critical infrastructure owners and operators for the purpose of receiving consensus policy advice and/or recommendations. The CIPAC review and forthcoming Sector Risk Management Plans, directed under NSM-22, are opportunities for government to improve its engagement with key stakeholders, including those in the subsea cable industry.

2. Streamline U.S. Permitting, Licensing, and Regulatory Processes

The fragmented regulatory landscape for subsea cables, coupled with increasing permitting timelines and unpredictability, have had real impact on the nation's attractiveness for investment into new cable systems. In order to ensure the United States remains a leader in the subsea cable industry and maintains its national security objectives through continued capacity growth, the regulatory landscape for deploying new cable systems should be predictable, reliable, and transparent. The federal government's interaction with the cable industry would benefit from improved internal coordination, as it has lacked the guidance of a shared strategic perspective with specific national and economic security objectives.

Path Forward: DHS will conduct a comprehensive assessment of cable permitting and licensing authorities—with an initial focus on federal authorities—to inform efforts to reduce unnecessary redundancy, clarify reporting requirements, and align resources to policy priorities. Working with federal and SLTT partners, DHS will evaluate best practices for coastal cable risk management, including nearshore seabed use, maritime coordination and

security, and cable landing station security and resilience. Through its role in Team Telecom, and in support of ongoing regulatory updates initiated in November 2024 by the FCC, DHS will pursue and support opportunities to enable faster, more transparent, and more consistent outcomes of FCC cable licensing through enhanced but predictable security and resilience requirements.

Enhancing the overall reliability and predictability of government licensing and permitting processes is key to achieving the United States' interests in maintaining a leadership role in the subsea cable industry. Doing so will ensure a secure and resilient cable infrastructure and promote a healthy investment environment that supports our national economic and security priorities.

3. Clarify Federal Roles and Responsibilities in Emergency Management and Incident Response

DHS acknowledges industry's request for clarity on the correct points of contact for incidents that invoke various U.S. government stakeholders or that overwhelm industry's independent ability to maintain or restore the nation's connectivity. Currently, federal responsibilities for cable protection, outage reporting, threat intelligence sharing, direct cable operations, and crisis response are coordinated through a variety of mechanisms across multiple departments and agencies. A clear concept of operations and defined lines of effort in cases of emergency has not been relayed to industry in a meaningful or collaborative way.

Path forward: Effective emergency management is built on effective planning, and NSM-22 directs CISA, as National Coordinator and SRMA for both the Communications and Information Technology sectors, to support domestic incident management, emergency preparedness, and national continuity. As part of its ongoing efforts in fulfilling this responsibility, DHS will lead the development of a joint overview of the U.S. government's operational authorities for subsea cable security and resilience, in support of an interagency concept of operations for partnering with industry owners and operators to secure and repair subsea cable systems in a variety of crisis scenarios.

Further, DHS will develop strategies to collaborate closely with federal partners and the subsea cable industry to review cable incidents and analyze industry-wide data on outages in an effort to uncover trends, refine attribution of causes, identify high-risk areas, and inform future risk mitigation efforts to reduce damage to submarine cable systems.

ENDNOTES

1 Alan Mauldin, *Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?*, TeleGeography (May 4, 2023), https://blog.telegeography.com/2023-mythbusting-part-3.

2 Sabine Siebold, *NATO says Moscow may sabotage undersea cables part of war on Ukraine, Reuters* (May 3, 2023), https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/.

3 42 U.S.C. § 5195(c).

4 62 Fed. Reg. 62,754 (Nov. 25, 1997).

5 6 U.S.C. § 652(c)(4).

6 Presidential Nat'l Sec. Mem. No. 10 (Apr. 30, 2024).

7 Exec. Order No. 13,913, 85 Fed. Reg. 19,643 (Apr. 4, 2020).

8 TeleGeography, *Submarine Cable Frequently Asked Questions*, (2024) https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions (last visited Dec. 5, 2024).

9 *Id.*

10 *David Gritten, Crucial Red Sea Data Cables Cut, Telecoms Firm Says*, BBC (Mar. 5, 2024), https://www.bbc.com/news/world-middle-east-68478828 (last visited Dec. 5, 2024).

11 Jeanne-Mây Desurmont, *Territorial Claims and Subsea Cables: The Geopolitics of Invisible Lines in the South China Sea*, BLOOMSBURY INTELLIGENCE & SEC. INST. (May 21, 2024).

12 Kristin Carlson, *The State of the Network: 2023 Edition*, TeleGeography (Feb. 13, 2023), https://www2.telegeography.com/download-state-of-the-network.

13 International Cable Protection Committee, *Cableships of the World*, (Nov, 25, 2024) https://www.iscpc.org/information/cableships-of-the-world/?page=1&items=10 (last visited Dec. 5, 2024).; Josh Dzieza, *The Cloud Under The Sea*, The Verge (Apr. 16, 2024). https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships (last visited Dec. 5, 2024).; Captain Douglas R. Burnett, USN (R) & Kristin Berdan, *To Secure Undersea Cables, Take Lessons from the British Empire's All-Red Line*, U.S. Naval Institute (Jul. 2024). https://www.usni.org/magazines/proceedings/2024/july/secure-undersea-cables-take-lessons-british-empires-all-red-line#:~:text=Today%2C%20there%20are%20only%20two,of%20%245%20million%20per%20vessel (last visited Dec. 5, 2024).

14 Sector Coordinating Councils (SCCs) are self-organized, self-run, and self-governed councils that enable critical infrastructure owners and operators and representative trade or equivalent associations to interact on a wide range of sector-specific strategies, policies, activities, and issues. Government Coordinating Councils (GCCs), chaired by the identified Sector Risk Management Agency, are formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCCs are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector.