WESTERN HEMISPHERE READINESS SERIES

HRS Resilience Foundation

TECHNICAL PAPER 04

Trusted-Supplier and Cable-Landing Review Frameworks for Submarine Cables

Scope, Criteria, Decision Rights and Assurance in the Western Hemisphere

PUBLICATION TYPE	PRIMARY ENVIRONMENT	EDITION
Independent technical paper	Western Hemisphere	October 2026

SERIES POSITION	AUTHOR	INSTITUTION
Technical Paper 04	André Vieira	HRS Resilience Foundation

Research integrity. Public research publication. Independent analysis. No U.S. Government endorsement or sponsorship. Not a procurement request, an endorsement of a vendor, or a representation of partnership with any government or private organization.

Evidence discipline. This publication presents an analytical framework. It does not represent the views, positions, endorsements or commitments of any government, international organization, university, donor or private company. It is not a legal opinion on any country's law and does not assess any supplier or operator.

CONTENTS

— Executive Summary 3

— Key Findings and Recommendations 4

01 The Technical Problem 5

02 Review Architecture: From Application to Assurance 6

03 Three Regulatory Approaches 7

04 Define: The Object of Review 8

05 Disclose: Ownership, Control and Supply-Chain Information 9

06 Assess: Risk Criteria Applied to Any Applicant or Supplier 10

07 Decide: Decision Rights, Timelines and Mitigation 11

08 Assure: Monitoring, Reporting and Periodic Review 12

09 Applied Case: Chile, 2026 13

10 Regional Instruments: Brazil, Peru and Mercosur 14

11 Performance Measurement and Design Checklist 15

12 Policy Relevance and Durability Protocol 16

13 Conclusion 17

— Selected References 18

About this series. This Technical Paper is the fourth publication in the HRS Resilience Foundation's Technical Paper series. It extends the framework approach introduced in Technical Paper 03[25] from port concessions to the review of submarine cable landings and trusted-supplier criteria, follows from Policy Brief 04[26], and draws on the applied case examined in Country Readiness Assessment 09 (Chile)[23] and on Sector Readiness Assessment 01.[24]

EXECUTIVE SUMMARY

Trusted-Supplier and Cable-Landing Review Frameworks for Submarine Cables

Submarine cables carry most international data traffic. The State Department has put the share at more than 95 percent of the world's digital traffic,[5] and Brazil's telecommunications regulator puts it at about 99 percent of Brazil's international data.[15] On 22 September 2026, fifteen governments, including Chile and Peru, stated their intention to promote trusted-supplier regulations for digital infrastructure applied on a non-discriminatory basis.[19] The statement is a declaration of intent; the procedures are left to each government.

Existing regimes answer the procedural question differently. The United States, in rules effective in November 2025, presumes that applicants owned or controlled by, or subject to the jurisdiction or direction of, a designated foreign adversary are not qualified to hold a cable landing license, and that landing a cable in a foreign adversary country warrants denial.[1] In June 2026 the FCC adopted a Second Report and Order that would license the owners and operators of submarine line terminal equipment (SLTE) and presumptively exempt from inter-agency referral any application that certifies ten national security standards; these and other provisions of the order await Office of Management and Budget review before taking effect.[22] The European Union's Cable Security Toolbox of early 2026 rests on a coordinated risk assessment, recommends reducing exposure to non-EU suppliers, and is non-binding for Member States.[7] Brazil's regulator opened a call for input (*tomada de subsídios*) on a cable regulatory framework in May 2026.[15] In Chile, two cables followed different institutional pathways in 2026: a decree on the Chile-China Express cable was withdrawn two days after it was signed, while the Humboldt cable, in which the Chilean state is a partner, was approved by the regional coastal-use commission.[9][10][12]

This paper develops the HRS Cable-Landing Assurance Framework, which structures a review in five stages: Define, Disclose, Assess, Decide and Assure. It proposes a criteria-based core that applies to any applicant or supplier and can treat another government's designation as evidence without depending on it. The framework is an analytical construct, not a legal opinion on any country's law, and takes no position on any supplier or cable.

> CENTRAL TECHNICAL PROPOSITION
>
> *A cable-landing review is trustworthy when its object is defined (Define), its inputs are disclosed (Disclose), its criteria are published and applied to every applicant (Assess), its decision has an owner and a clock (Decide), and its outcome is monitored after the cable lands (Assure).*

KEY FINDINGS AND RECOMMENDATIONS

Key Findings and Recommendations

Five findings from the regimes and cases examined, each paired with a recommendation that applies to any government reviewing a cable landing.

Key Finding	Recommendation
Regimes differ in kind: the U.S. rules are designation-based and, from 2026, add a certification route; the EU toolbox pairs a risk assessment with a preference for EU supply, and the Joint Statement's trusted-supplier language is non-discriminatory.[1][7][19][22]	Build a criteria-based core that applies to every applicant, and treat allied designations as admissible evidence rather than automatic outcomes.
Reviews are only as complete as their object: the U.S. rules define a "submarine cable system" and license entities that control a landing station, and the EU toolbox extends to dry plant and repair vessels.[1][7]	Define the review object to include landing stations, operations centres, dry plant, the repair chain and third-party providers.
Risk can be assessed without reference to nationality: the EU toolbox records that more than 90 percent of transatlantic capacity is wholly or partly owned by U.S.-based hyperscalers, and Brazil's regulator flags concentrated landing points.[7][15]	Include control, legal exposure, remote access, supply continuity and concentration among published criteria.
Process certainty matters: before 2020 the U.S. review had no published clock and one application took from 2011 to 2019; Chile's decree was withdrawn in two days.[3][4][10]	Name a decision owner, publish the clock and use standard mitigation instruments.
In 2026 two Chilean cables followed different pathways, and the state is itself a partner in one of them.[12][13][14]	Apply the same published criteria to every cable and separate the reviewer from any state entity that invests.

SECTION 01

The Technical Problem

A cable-landing decision touches four things at once: the physical system, the facilities where it lands and is managed, the companies that own and supply it, and the traffic it carries. Reviews fail when any of these is left outside the procedure, when the inputs are not disclosed, when the clock is undefined, or when the same standards are not applied to every cable. Each failure mode below has a documented counterpart in a regime or a case examined in this paper.

Failure Mode	Illustrative Mechanism
Undefined object	The review covers the cable but not the landing station, the operations centre or the repair chain; the U.S. rules had to define "submarine cable system" and tie licensing to control of the landing station, and in 2026 adopted licensing for the owners and operators of terminal equipment (SLTE), pending Office of Management and Budget review.[1][22]
Undisclosed control or access	Ownership, remote-access and supply arrangements are not visible to the reviewer; the EU's risk scenarios include backdoor access enabling a malicious shutdown.[7]
Undefined clock	Before 2020 the U.S. inter-agency review had no set timing mandates, and one application was filed in 2011 and denied in 2019; Chile's decree was withdrawn two days after signing.[3][4][10]
Unexamined concentration	Routes, landing points or capacity ownership are concentrated; Brazil's landing points cluster in four hubs, and the EU toolbox records that, as of 2025, more than 90 percent of transatlantic capacity was wholly or partly owned by U.S.-based hyperscalers.[7][15]
Inconsistent pathways	Two cables in the same country are processed through different institutions and on different timelines (Chile, 2026).[10][12]
Post-landing blind spot	Nothing is reported or re-reviewed after approval; the U.S. rules add an annual report, and Brazil's cybersecurity regulation requires incident reporting by international cable operators.[1][17]

Scope note: This paper presents an analytical framework, not a legal opinion on any country's law, and it does not assess any supplier, operator or cable. Regimes are described as of early October 2026 from public sources: the U.S. rules through the Federal Register notices for FCC 25-49 and FCC 26-42, the EU toolbox and the Expert Group's risk assessment through their published texts, and the Mercosur recommendation through its official text. Pending processes in Chile and Brazil may have changed.

SECTION 02

Review Architecture: From Application to Assurance

The HRS Cable-Landing Assurance Framework treats the review of a cable landing as five linked stages. Each stage should have a decision right, a public record and a time-based indicator. The stages continue after approval: the output of Assure feeds the next Define.

Stage	Function	Case Illustration
1. Define	Fix the object of review: the cable system, landing station, operations centre and dry plant, repair chain and third-party providers.	The U.S. rules adopt a definition of "submarine cable system" and require entities that control a landing station to hold licenses; a 2026 order adopts licensing for SLTE owners and operators, not yet in effect.[1][22] The EU toolbox covers beach manholes, landing stations and depots.[7]
2. Disclose	Require standard information on ownership, control, supply chain and remote access.	Certain U.S. licensees file an annual report on ownership and operations; the EU toolbox recommends assessing suppliers' profile and dependencies.[1][7]
3. Assess	Apply published risk criteria to any applicant or supplier.	The EU toolbox derives seven risk scenarios from 28 threats, 16 vulnerabilities and 23 dependencies.[7]
4. Decide	Name the decision owner, publish the clock and standardize mitigation.	U.S. Executive Order 13913 sets a 120-day initial review and a secondary assessment of up to 90 days; mitigation is recorded in a Letter of Agreement or National Security Agreement.[3][4] FCC 26-42 adopts ten published standards that would exempt qualifying applications from referral once in effect.[22]
5. Assure	Monitor, report and re-review after the cable lands.	U.S. annual reporting; Brazil's cybersecurity regulation covers incident reporting by international cable operators.[1][17]

TECHNICAL NOTE

The stages are only as strong as their inputs: an Assess stage cannot test an ownership chain that Disclose never collected, and a Decide stage cannot be defended if its clock and criteria were not published before the application arrived.

SECTION 03

Three Regulatory Approaches

Three approaches to trusted-supplier and cable-landing review can be distinguished in the regimes examined. They are not exclusive, and no regime is a pure example of one.

Approach	Example	Mechanism	Strength and Limit
Designation-based	U.S. FCC rules, 2025–2026	Presumptions tied to designated foreign adversaries and to the FCC's Covered List; a presumption against landing a cable in a foreign adversary country.[1] A 2026 order adopts a certification route: applications that meet ten published national security standards would be presumptively exempt from referral once the provision takes effect.[22]	Clear and fast to apply; depends on a designation list that partners may not share.
Risk assessment with origin preference	EU Cable Security Toolbox, 2026	Coordinated risk assessment; recommends assessing supply-chain dependencies and reducing exposure to non-EU suppliers; cable-project funding excludes suppliers identified as high-risk.[7]	Anchored in documented risk scenarios; the origin preference may not transfer to partners without a regional supply base, and the measures are non-binding.
Neutral criteria	Joint Statement language; OECD non-discrimination principle	Published risk criteria applied to every applicant and supplier, whatever its nationality.[19][20]	Legally defensible and acceptable to partners with different external relationships; requires analytical capacity and evidence.

TECHNICAL NOTE

A criteria-based core can treat another government's designation as evidence in a specific review without making it the outcome. The Joint Statement's non-discrimination clause attaches to trusted-supplier regulations for digital infrastructure; this paper applies the same principle to cable-landing review as a design choice, not because the statement requires it.[19]

SECTION 04

Define: The Object of Review

A review can only be as complete as its object. The U.S. rules show the point: they adopt a definition of "submarine cable system" that acknowledges technological change and require any entity that controls a cable landing station to be an applicant for, and licensee on, a cable landing license, while entities that merely own the station no longer must.[1] In 2026 the FCC went further and adopted licensing for the owners and operators of submarine line terminal equipment (SLTE), a measure delayed pending Office of Management and Budget review.[22] Brazil's regulator took a more incremental step in 2024, extending its cybersecurity regulation to international submarine cable operators.[17]

Object	Why It Is in Scope	Anchor
Cable system (wet plant and terminal equipment)	The asset that carries traffic.	Definition of "submarine cable system"[1]
Landing station and beach manhole	The physical entry point; whoever controls the station controls the landing.	Licensing of entities that control a landing station; protection of the beach manhole and station[1][7]
SLTE owners and operators	The equipment that lights the cable; whoever owns or operates it can affect how the system operates, whether or not it holds an interest in the cable.	FCC 26-42 licensing of SLTE owners and operators (adopted; delayed pending OMB review)[22]
Operations centre and dry plant	Remote management and power feeding determine availability and access.	EU measure on dry-plant security and power resilience[7]
Repair vessels, depots and spares	Repair capacity is a dependency; the EU toolbox recommends scrutinising acquisitions of vessels and depots.	EU strategic measure on maintenance and repair; [7] U.S. exemption for wet-segment repair, granted because specialised repair ships are scarce (adopted; delayed with the related conditions)[22]
Third-party and managed services	Remote access can sit outside the licensee.	EU risk scenario on backdoor access;[7] FCC 26-42 conditions on third-party service providers (adopted; delayed pending OMB review)[22]

SECTION 05

Disclose: Ownership, Control and Supply-Chain Information

Disclosure turns a review from a judgment about a company's reputation into a judgment about documented facts. It should be standardized, so that the same form serves every applicant. The U.S. Office of Management and Budget approved new FCC forms on 26 June 2026, including a Foreign Adversary Annual Report and certifications on the Covered List and on cybersecurity and physical security risk-management plans, which shows how disclosure can be made routine.[2]

Disclosure Item	Purpose	Anchor
Ownership and control chain to the ultimate controller, including any government or state ownership	Identify who decides and who can be compelled.	U.S. annual report on licensee and system ownership; OECD work on government-controlled investors[1][21]
Supplier and maintenance chain	Identify dependencies in components, updates and repair.	EU measure on supply-chain dependencies[7]
Remote-access and update arrangements	Identify who can access, modify or disable the system.	EU risk scenario on backdoor access[7]
Landing and routing plan	Assess resilience and concentration.	EU measure on route and landing diversity; Brazil's concern with landing-point concentration[7][15]
Cyber and physical security plan	Establish a baseline that can be audited.	U.S. certification of a risk-management plan[1]
Changes after approval	Trigger re-review.	U.S. rules on changes in ownership[1]

SECTION 06

Assess: Risk Criteria Applied to Any Applicant or Supplier

Each criterion below is a question that can be asked of any applicant or supplier, whatever its nationality. A criteria-based review can still produce different results for different applicants, because the facts differ. The criteria draw on the risk scenarios of the EU assessment and on the questions the U.S. rules ask.[1][7]

Criterion	Question Asked	Anchor
1. Ownership and control	Who ultimately owns or controls the system, and does any government or state entity, of any nationality, hold control?	U.S. test of ownership and control; OECD work on government-controlled investors[1][21]
2. Legal exposure	Can any government compel the applicant or supplier to provide access, data or assistance, and under what law?	U.S. test of subjection to a foreign government's jurisdiction or direction; EU scenario on interference with a supplier[1][7]
3. Remote access	Who can access, modify or shut down the system remotely, and can this be audited?	EU scenario on backdoor access[7]
4. Supply continuity	Could the supply of components, updates or repair be blocked or conditioned?	EU scenario on blocked supply[7]
5. Concentration	How concentrated are routes, landing points and capacity ownership?	EU measure on route diversity; Brazil's landing-point concern[7][15]
6. Protection and repair capability	Are physical and cyber protection, power resilience and repair capacity adequate?	EU technical measures; U.S. security certification[1][7]
7. Track record and transparency	Is the applicant's disclosure complete and its record reliable?	EU supplier-profile assessment[7]

SECTION 07

Decide: Decision Rights, Timelines and Mitigation

Before Executive Order 13913 of April 2020, the U.S. inter-agency review of telecommunications licenses had no set timing mandates, and a China Mobile USA application for international Section 214 authority, filed in 2011, was denied in 2019 after the Executive Branch agencies recommended denial.[3][4] The order created a committee chaired by the Attorney General's department, a 120-day initial review and a secondary assessment of up to 90 days, and limited its powers to recommending that the FCC dismiss, deny, condition, modify or revoke a license.[3][4] The lesson for partners is procedural: the value of a clock and a standard outcome set is independent of which criteria a government adopts.

The U.S. model has since moved from case-by-case referral toward published standards. FCC 26-42 would presumptively exempt from referral applications that certify ten national security standards, and would exclude certain renewals when the same cable was reviewed within the previous three years. The 120-day and 90-day clock therefore governs the applications that are referred. The exemption is adopted but not yet in effect.[22]

Decision Element	Standard	Example
Decision owner	One authority decides, after consultation with security, foreign-affairs and maritime authorities.	In the U.S. the FCC decides on the committee's recommendation; Brazil's regulator is considering a single window for cables.[3][17]
Published clock	A fixed initial review period and a defined extension.	120 days for the initial review after the Chair finds the application complete, plus up to 90 days for a secondary assessment.[3][4]
Outcomes and reasons	Approve, approve with conditions or deny, with reasons recorded.	The committee's recommendation options under the order.[3]
Standard mitigation	Pre-defined conditions in a standard instrument.	Letters of Agreement and National Security Agreements, the latter now typical for cable matters;[4] FCC 26-42 adopts ten published standards that an applicant could certify once in effect.[22]
Independence	The reviewer is separate from any state entity that invests in the cable.	In Chile the state developer Desarrollo País holds 50 percent of Humboldt Connect, the joint venture that holds two of the Humboldt cable's 16 fibre pairs; regional reports on the 2026 approval describe the US$11.5 million project submitted for approval as 99 percent funded by Google.[13][14][12]

SECTION 08

Assure: Monitoring, Reporting and Periodic Review

Assurance is where reviews are most often thin. The U.S. rules add an annual report for certain licensees and address changes in ownership;[1] Executive Order 13913 allows the committee to review existing licenses and mitigation agreements for new risks;[3][4] and Brazil's cybersecurity regulation covers incident reporting by international cable operators.[17] The EU toolbox adds exercises that include the repair dimension and monitoring technologies on the cables themselves.[7] The exemption standards adopted in FCC 26-42, not yet in effect, would by contrast require advance notice and committee non-objection before sensing capabilities such as distributed acoustic sensing are tested or added.[22]

Assurance Element	Standard	Example
Periodic reporting	Annual information on ownership, operations and changes.	U.S. Foreign Adversary Annual Report.[1][2]
Incident reporting	Cyber and physical incidents reported to the regulator.	Brazil's cybersecurity regulation for international cable operators;[17] 72-hour notice under the FCC 26-42 standards (not yet in effect).[22]
Change-of-control triggers	Re-review when ownership or control changes.	U.S. rules on changes in ownership.[1]
Continuing conditions	Conditions and audits that stay attached to an approval, including one granted without referral.	FCC 26-42 standards (not yet in effect): annual compliance report, consent to inspection and periodic third-party audit on request.[22]
Exercises and readiness	Joint exercises with operators, including repair.	EU measures on repair capacity and coordination.[7]
Monitoring and detection	Surveillance on the cable and its approaches.	EU measure on distributed acoustic sensing and smart cables.[7]
Periodic re-review	Scheduled re-examination of approved cables and conditions.	Review of existing licenses under the order.[3][4]

SECTION 09

Applied Case: Chile, 2026

Chile offers a documented 2026 comparison of two cables processed through different pathways. This paper takes no position on either cable; it asks what the framework would require of both.

Date	Event	Source
June 2025	Desarrollo País, a state-owned developer, and Google create Humboldt Connect, a 50-50 joint venture for the Humboldt cable (about 14,800 km, from the Valparaíso region to Sydney via French Polynesia). Google holds 14 of the cable's 16 fibre pairs and the joint venture holds the other two; commercial operation was announced for 2027.	[13] [14]
January 2026	The minister signs a decree granting a 30-year concession to China Mobile International's Chilean subsidiary for the Chile-China Express cable (reported investment of about US$500 million). The decree had not yet been sent to the Comptroller, and the government later described it as an early administrative step with no definitive approval. It is annulled on 29 January: the written request cites a technical error, and the minister later said he reversed it after receiving security information from the U.S. embassy.	[9][10]
February 2026	The United States revokes the visas of three Chilean officials, saying their activities compromised critical telecommunications infrastructure and regional security.	[9]
Mid-2026	The new government places the Chile-China Express project on hold; Subtel tells a transparency request that no definitive administrative resolution has been adopted on the possible concession.	[12]
June 2026	The regional coastal-use commission unanimously approves installation and operation of the Humboldt system: two cables from Santo Domingo, one to Sydney and one to Panama City, more than 21,000 km in total. Physical deployment is expected to begin at the end of 2026; reports on the approval now give 2028 for commercial operation, against the 2027 announced in 2025.	[12]

Stage	Question the Framework Asks of Both Cables
Define	What was the object of review for each cable: the cable, the landing station, the operations centre, the repair chain?
Disclose	What ownership, control, supply-chain and remote-access information was required, on the same form?
Assess	Which published criteria were applied, and were they the same for both?
Decide	Which authority decided, under what clock, with what reasons recorded, and does the state's role as a partner in one cable change who reviews?
Assure	What reporting and re-review apply after approval?

Public reporting does not describe a common published procedure applied to both cables; this paper did not locate one. [10][11]

SECTION 10

Regional Instruments: Brazil, Peru and Mercosur

Brazil's regulator reports that cables carry about 99 percent of the country's international data traffic and that landing points are concentrated in Fortaleza, Rio de Janeiro, Praia Grande and Santos.[15] Its board approved on 12 February 2026 the inclusion of a project to consolidate and update cable rules in its regulatory agenda; a call for input (*tomada de subsídios*) opened on 26 May 2026, its deadline was extended to 31 July, and the impact analysis is expected by the end of 2026.[15][16] The call for input asks about minimum physical and cyber security requirements, monitoring, certification and authorization models, and the concentration of landing points.[15] A draft 2027–2028 agenda, open for public consultation until 3 August 2026, lists the consolidation of cable rules again.[16]

Jurisdiction	Instrument	Status at Cutoff	Gap Through the Framework Lens
Brazil	Anatel cybersecurity regulation extended to international cable operators in 2024; project on cable rules in the 2025–2026 regulatory agenda, which a draft 2027–2028 agenda carries forward.[16][17]	Call for input; impact analysis pending	Certification and authorization models and a single window are under study.
Peru	Authorization by the Ministry of Transport and Communications for the landing and operation of cables.[18]	In force	The general telecommunications regulation lets the Ministry deny any concession or authorization that endangers national security or the public interest;[18] this paper did not locate a cable-specific security-review step or timeline.
Chile	Telecommunications concession process and regional coastal-use approval (Section 09).[10][12]	Two pathways in 2026	No common published procedure located.
Mercosur	Recommendation MERCOSUL/CMC/REC. N° 01/25 on the security and resilience of submarine cable infrastructure, adopted by the Common Market Council on 3 July 2025.[17]	Adopted	Recommends that States Parties assess and map cable risks, cooperate on incident response and repair, invest, train specialists, harmonize security norms, secure route redundancy, ensure contingency plans by owners and operators and raise awareness. As a recommendation it sets no review procedure for landings.

SECTION 11

Performance Measurement and Design Checklist

Cable-review governance should be measured by how fully and how predictably each stage operates, not by how many cables are approved or refused.

Indicator	What It Measures
Scope coverage	Share of cable-related facilities (landing stations, operations centres, depots) inside the review scope.
Disclosure completeness	Share of applications filed with the full standard disclosure.
Cycle time	Days from a complete application to a reasoned decision.
Criteria publication	Whether the criteria are published and applied to every applicant.
Assurance compliance	Share of licensees filing periodic and incident reports on time.
Concentration	Share of international capacity through the three largest landing points or owners.

Element	Design Question
Scope	Does the review cover landing stations, operations centres, the repair chain and third-party providers?
Disclosure	Is there one standard form for ownership, control, supply chain and remote access?
Criteria	Are the criteria published, identical for every applicant and evidence-based?
Decision owner and clock	Is there a single accountable authority and a published review period?
Independence	Is the reviewer separate from any state entity that invests in the cable?
Assurance	Do reporting, incident notification and re-review continue after approval?

SECTION 12

Policy Relevance and Durability Protocol

This section links the framework to commitments and measures already in place, and sets out how the paper is meant to be kept current. The nationality-neutral core of the framework is HRS's own design choice; it is offered so that any partner government can adopt a review procedure without presupposing a position on any particular supplier.

Initiative	Status	Relevance to the Framework
Joint Statement on Defending Hemispheric Sovereignty, 22 September 2026	Fifteen governments, including Chile and Peru, stated their intention to promote trusted-supplier regulations for digital infrastructure applied on a non-discriminatory basis.[19]	The five stages give that commitment a procedural form for submarine cables.
FCC Report and Order 25-49 and Second Report and Order 26-42	First order: rules generally effective 26 November 2025; the remaining rules, after OMB approval of 26 June 2026, took effect on 8 July 2026, including the Foreign Adversary Annual Report.[1][2] Second order: adopted 25 June 2026 and published 27 July 2026; general rules effective 25 September 2026, while specified provisions (SLTE licensing, new certifications and conditions, and the referral exemption) remain delayed pending OMB review and a further effective-date notice.[22]	The FCC's standardized forms and published standards give partner regimes a model for routine disclosure and a format they can recognize.
Strategic Subsea Cables Act of 2026 (Wilson, R-SC; Meeks, D-NY)	Bipartisan bill (H.R. 8069) introduced in March 2026; it would require at least two dedicated, full-time State Department staff and a presidential inter-agency committee; this paper did not locate evidence of enactment.[6]	Bipartisan interest in State Department capacity on cables, which a named decision owner and partner engagement require.
EU Cable Security Toolbox	Presented 5 February 2026 with about EUR 347 million for cable projects; its measures are non-binding.[7][8]	A comparable reference for risk scenarios and mitigation measures.

The paper has two layers. The framework layer (Sections 02 to 08 and 11) is structural and designed to remain valid across changes of government; with the object table adapted, it applies to other cross-border digital infrastructure. The case layer (Sections 01, 09 and 10) records processes as of early October 2026 and will age. The paper is revised when a trigger below occurs: the case layer is updated, and the framework layer changes only if a trigger exposes a design flaw.

Watch Item	Status at Cutoff	Update Trigger
Chile-China Express	On hold, as reported	A decision to proceed, reject or formalize a review procedure
Humboldt cable	Approved; physical deployment expected at the end of 2026	Start of deployment or a change in the review pathway
Brazil's cable rules	Impact analysis expected by end-2026; also in the draft 2027–2028 agenda	Publication of a draft rule or of the analysis
Strategic Subsea Cables Act of 2026	Introduced; enactment not located	Committee action or enactment
FCC 26-42 delayed provisions (SLTE licensing, certifications, referral exemption)	Adopted; delayed pending OMB review	Federal Register notice announcing the effective date

Version control: V1.0, October 2026. Scheduled review after 31 December 2026 (end of Brazil's 2025–2026 agenda, which schedules the impact analysis; a draft 2027–2028 agenda lists the topic) and no later than April 2027, or earlier on any trigger above.[16]

SECTION 13

Conclusion

The regimes and cases examined do not disagree about the need for review; they differ in who decides, on what criteria and by when. The United States relies on designations and has adopted, in 2026, a route based on certifiable standards; the European Union relies on a coordinated risk assessment with a preference for EU supply; and the partner governments examined are earlier in the process: Brazil is gathering input on a framework, Peru authorizes landings through its ministry, and Chile processed two cables through different pathways in 2026.[1][7][12][15][18][22]

The HRS Cable-Landing Assurance Framework (Define, Disclose, Assess, Decide and Assure) offers a procedural form that works whichever approach a government prefers, because its stages concern the quality of the process rather than the identity of the supplier. A review that is defined, disclosed, criteria-based, owned and monitored is easier to defend to investors, to partners and to a successor government.

> CLOSING TECHNICAL NOTE
>
> *A review procedure is not a verdict on any supplier; it is the means by which a government can reach, explain and defend a verdict before a transaction, a diplomatic episode or an outage forces the question.*

SELECTED REFERENCES

Selected References

Web sources accessed October 2026.

[1] Federal Communications Commission. Review of Submarine Cable Landing License Rules and Procedures, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-49 (OI Docket 24-524), adopted 7 August 2025; Federal Register notice of 27 October 2025 (rules effective 26 November 2025). docs.fcc.gov/public/attachments/FCC-25-49A1.pdf; federalregister.gov/documents/2025/10/27/2025-19658/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security

[2] Federal Communications Commission. Review of Submarine Cable Landing License Rules and Procedures, final rule, announcement of effective date, Federal Register notice 2026-13765 (OMB approval of 26 June 2026 for the Foreign Adversary Annual Report and one-time certifications); FCC Office of International Affairs, DA 26-684 (rules not in effect on 26 November 2025 became effective on 8 July 2026). federalregister.gov/d/2026-13765; docs.fcc.gov/public/attachments/DA-26-684A1.pdf

[3] The White House. Executive Order 13913, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 4 April 2020. govinfo.gov/content/pkg/DCPD-202000242/html/DCPD-202000242.htm

[4] Skadden, Executive Order Seeks to Modernize "Team Telecom" After Years-Long Effort (April 2020); hlc.com, Team Telecom officials demystify investment review process in panel discussion. skadden.com/insights/publications/2020/04/executive-order-seeks-to-modernize; hlc.com/en/publications/team-telecom-officials-demystify-investment-review-process-in-panel-discussion

[5] U.S. Department of State. United States International Cyberspace & Digital Policy Strategy, May 2024, Line of Effort 3 (undersea cables carry more than 95 percent of the world's digital traffic); MeriTalk, State Department prioritizing undersea cable security push (2024). meritalk.com/articles/state-dept-prioritizing-undersea-cable-security-push/

[6] Office of Rep. Joe Wilson. Wilson and Meeks Introduce Strategic Subsea Cables Act of 2026. 27 March 2026. joewilson.house.gov/media/press-releases/wilson-and-meeks-introduce-strategic-subsea-cables-act-2026; H.R. 8069, 119th Cong. (introduced 24 March 2026), govinfo.gov/app/details/BILLS-119hr8069ih

[7] Submarine Cable Infrastructures Expert Group (European Commission, Member States and ENISA). Cable Security Toolbox of Mitigation Measures and Cable Projects of European Interest, version 5, 19 January 2026 (copy hosted by Bulgaria's Ministry of Transport and Communications), mtc.government.bg/sites/default/files/documents/2026-02/Submarine%20Cable%20Toolbox.pdf; and Security and Resilience of EU Submarine Cable Infrastructures: Mapping, Risk Assessments, Stress Tests, October 2025, digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures

[8] European Commission, Blue Economy Observatory. EUR 347 million to protect Europe's submarine cables. February 2026. blue-economy-observatory.ec.europa.eu/news/eu347-million-protect-europes-submarine-cables-2026-02-11_es

[9] Rest of World. Chile, China and the Google cable: the Chile-China Express dispute. 2026. restofworld.org/2026/chile-china-america-google-cable/

[10] 24horas.cl. Esta es la cronología del "cable chino" que tensiona la política chilena. 2026; Datacenter Dynamics (Brazil), Chile suspende cabo submarino chinês. 24horas.cl/actualidad/nacional/esta-es-la-cronologia-del-cable-chino-que-tensiona-politica-chilena

[11] Expansión (Mexico), 25 February 2026, citing El País. expansion.mx/mundo/2026/02/25/un-cable-submarino-que-conecta-con-china-esta-en-el-centro-de-la-disputa-entre-chile-y-eu

[12] Ex-Ante. Cómo avanza el cable submarino de Google con el Estado luego de que el Gobierno dejara el proyecto chino en el congelador. 2026. ex-ante.cl/?p=360683; El Desconcierto, 22 June 2026, eldesconcierto.cl/actualidad/chile-como-nodo-digital-america-y-asia-pacifico-aprueban-red-submarina-fibra-optica-21-mil-km-n5459833

[13] La Tercera. Desarrollo País y cable submarino con Google. 2024. latercera.com/pulso/noticia/desarrollo-pais-y-cable-submarino-con-google-nos-va-a-permitir-traer-tecnologia-del-mas-alto-estandar-para-transformar-a-chile-en-un-hub-digital/ASEBSL7LU5EEBLJOEA3QUW7ETY/

[14] DPL News. Chile y Google prometen operación comercial del cable submarino Humboldt en 2027. June 2025. dplnews.com/chile-google-operacion-cable-submarino-humboldt-2027/

[15] Poder360. Governo inicia discussão sobre regulação de cabos submarinos. 26 May 2026; DPL News, Anatel abre tomada de subsídios sobre cabos submarinos. poder360.com.br/poder-infra/governo-inicia-discussao-sobre-regulacao-de-cabos-submarinos/

[16] TeleTime. Anatel prorroga tomada de subsídios sobre cabos submarinos. 25 June 2026; Datacenter Dynamics (Brazil), Anatel atualizará regras para cabos submarinos (February 2026); Demarest, Anatel submete proposta de Agenda Regulatória 2027–2028 à consulta pública (22 June 2026). teletime.com.br/25/06/2026/cabos-submarinos-anatel/; demarest.com.br/anatel-submete-proposta-de-agenda-regulatoria-2027-2028-a-consulta-publica/

[17] MERCOSUR Common Market Council, MERCOSUR/CMC/REC. N° 01/25, Seguridad y Resiliencia de Infraestructuras de Cables Submarinos, LXVI CMC, Buenos Aires, 3 July 2025, normas.mercosur.int/simfiles/normativas/107695_REC_001-2025_ES_Seguridad%20Infraest%20cable%20submarinos.pdf; MobileTime, on Anatel Resolution 767/2024; Convergência Digital, Anatel vai apertar regulação e virar porta única para cabos submarinos. mobiletime.com.br/?p=860946; convergenciadigital.com.br/?p=49530

[18] Lex Mundi. Latin America and the Caribbean TMT and Cyber Guide: Peru. lexmundi.com/guides/lex-mundi-latin-america-and-the-caribbean-tmt-and-cyber-guide/jurisdictions/latin-america/peru/; Peru, Reglamento General de la Ley de Telecomunicaciones (TUO), D.S. 020-2007-MTC, art. 113. osiptel.gob.pe/media/kakhcv2n/ds020-2007-mtc.pdf

[19] U.S. Department of State, Office of the Spokesman. Joint Statement on Defending Hemispheric Sovereignty, 22 September 2026. state.gov/releases/office-of-the-spokesman/2026/09/joint-statement-on-defending-hemispheric-sovereignty/

[20] OECD. Guidelines for Recipient Country Investment Policies relating to National Security, OECD/LEGAL/0372. 2009. legalinstruments.oecd.org/public/doc/227/227.en.pdf

[21] OECD. Foreign government-controlled investors and recipient country investment policies: a scoping paper. OECD Working Papers on International Investment, 2009/01. oecd.org/en/publications/foreign-government-controlled-investors-and-recipient-country-investment-policies_80a729c7-en.html

[22] 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, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 26-42 (OI Docket No. 24-523; MD Docket No. 24-524), adopted 25 June 2026, released 30 June 2026; Federal Register notice of 27 July 2026, 91 FR 46844 (general rules effective 25 September 2026; specified provisions, including SLTE licensing and the referral exemption, delayed pending OMB review). docs.fcc.gov/public/attachments/FCC-26-42A1.pdf; federalregister.gov/d/2026-15123

[23] HRS Resilience Foundation. Country Readiness Assessment 09 — Chile: Institutional Readiness, Strategic Minerals and Hemispheric Realignment. September 2026.

[24] HRS Resilience Foundation. Sector Readiness Assessment 01 — Telecommunications & Digital Infrastructure. 2026.

[25] HRS Resilience Foundation. Technical Paper 03 — Concession Transparency Frameworks for Strategic Ports. October 2026.

[26] HRS Resilience Foundation. Policy Brief 04 — From Commitment to Capacity: What a State-Led Investment Screening Initiative Should Prioritize in the Western Hemisphere. October 2026.

WESTERN HEMISPHERE READINESS SERIES

HRS Resilience Foundation

Independent research for institutional readiness, continuity, and 50-year resilience planning across the Western Hemisphere. Research Outputs span Strategic Reports, Policy Briefs, Technical Papers, Sector Readiness Assessments and Country Assessments, translating public-source evidence into practical frameworks built to remain valid for governments, infrastructure operators, investors, and institutional decision-makers across changes in technology, suppliers, and political leadership.

RESEARCH OUTPUTS TO DATE

STRATEGIC REPORTS

Strategic Report 01 — Health Security and Institutional Resilience in the Americas

Strategic Report 02 — Resilient Infrastructure Investment in the Western Hemisphere

Strategic Report 03 — Strategic Dependency Patterns Across the Western Hemisphere

Strategic Report 04 — China's Bi-Oceanic Pivot: South American Land Corridors as a Panama Canal Alternative

POLICY BRIEFS

Policy Brief 01 — Strengthening Regional Health Emergency Readiness in the Americas

Policy Brief 02 — Operationalizing the Economic Pillar of the Shield of the Americas

Policy Brief 03 — Operationalizing the Security Pillar of the Shield of the Americas

Policy Brief 04 — From Commitment to Capacity: What a State-Led Investment Screening Initiative Should Prioritize in the Western Hemisphere

TECHNICAL PAPERS

Technical Paper 01 — Building Resilient Health Supply Chains

Technical Paper 02 — Fiscal Transparency Frameworks for Resource-Boom States

Technical Paper 03 — Concession Transparency Frameworks for Strategic Ports

Technical Paper 04 — Trusted-Supplier and Cable-Landing Review Frameworks for Submarine Cables

SECTOR ASSESSMENTS

SRA 01 — Telecommunications & Digital Infrastructure
SRA 02 — Data Centers, Cloud & AI Infrastructure
SRA 03 — Critical Minerals & Strategic Materials
SRA 04 — Rare Earths & Western Hemisphere Mineral Security
SRA 05 — Energy Security & Strategic Power Infrastructure
SRA 06 — Ports, Logistics & Maritime Infrastructure
SRA 07 — Food Security & Strategic Agricultural Resilience
SRA 08 — Pharmaceutical & Medical Supply Chains
SRA 09 — Advanced Manufacturing & Industrial Capacity
SRA 10 — Western Hemisphere Strategic Infrastructure & Resilience

COUNTRY ASSESSMENTS

Country Readiness Assessment 01 — Brazil
Country Readiness Assessment 02 — Venezuela
Country Readiness Assessment 03 — Cuba
Country Readiness Assessment 04 — Colombia
Country Readiness Assessment 05 — Bolivia
Country Readiness Assessment 06 — Peru
Country Readiness Assessment 07 — Ecuador
Country Readiness Assessment 08 — Paraguay
Country Readiness Assessment 09 — Chile
Country Readiness Assessment 10 — Argentina
Country Readiness Assessment 11 — Panama
Country Readiness Assessment 12 — Guyana

André Vieira, MD

FOUNDER & CHAIRMAN, HRS RESILIENCE FOUNDATION

© 2026 HRS Resilience Foundation. Western Hemisphere Readiness Series. All rights reserved. No U.S. Government or foreign-government endorsement is implied or claimed.