

Designing for Success:

How an Effective IP and Data-Sharing Framework
Helps Test Centers Unlock Geothermal Innovation

By Laura Katharina Mueller

Clean Air Task Force, in collaboration with the Cascade Institute

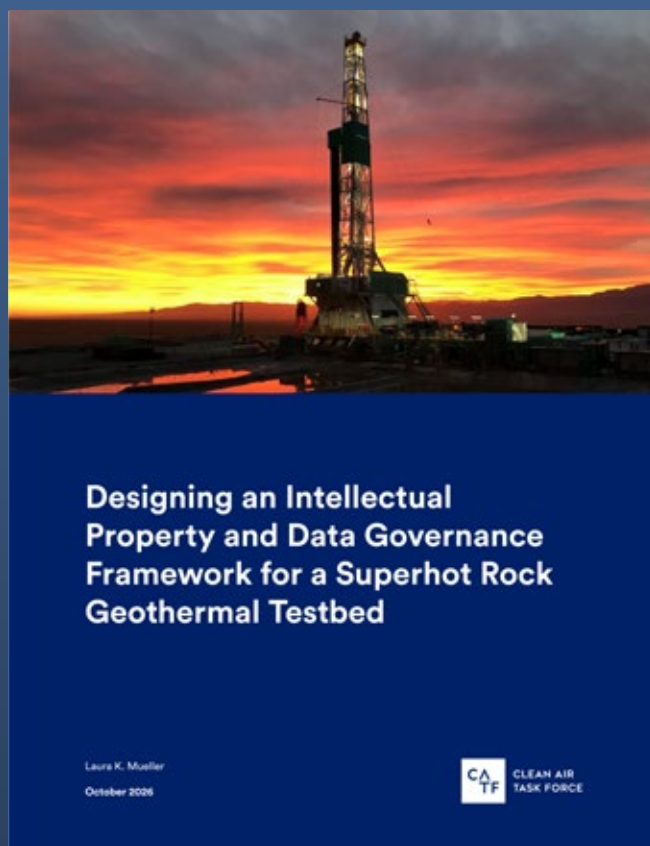
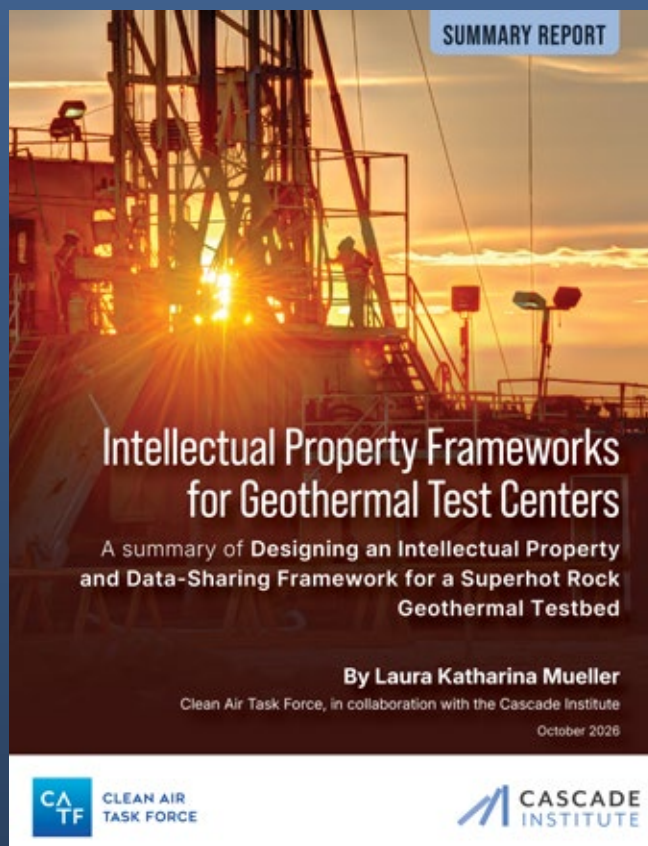
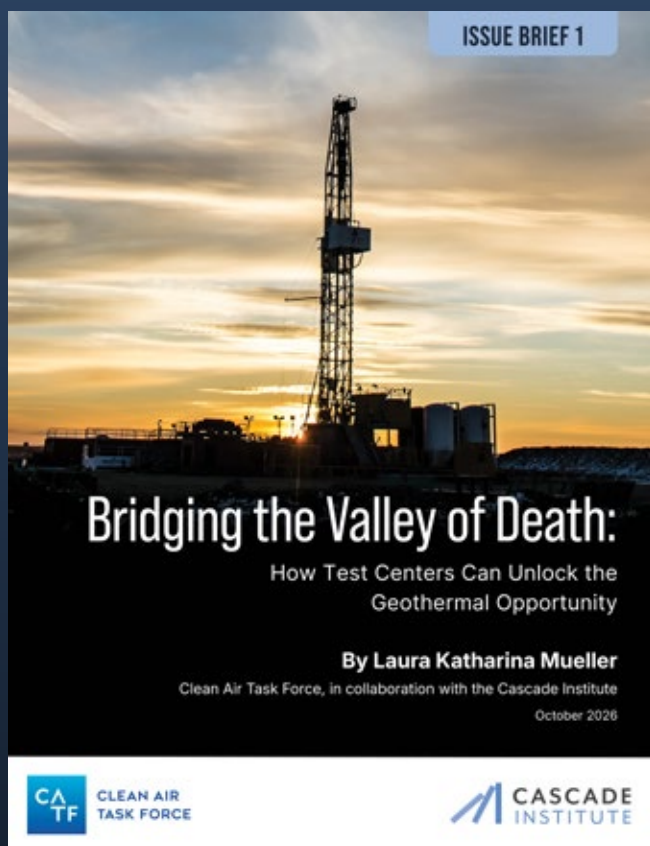
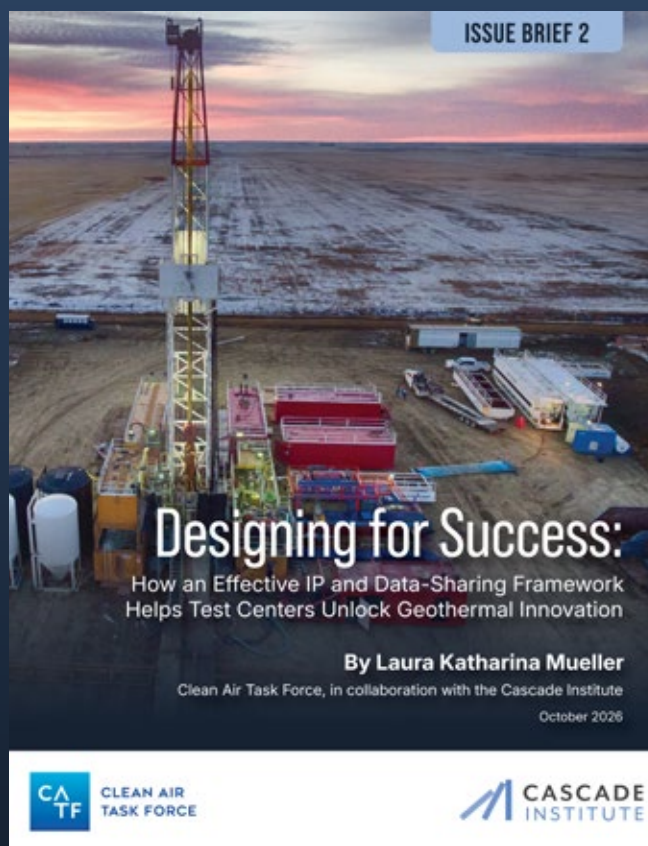
October 2026



CLEAN AIR
TASK FORCE



The full geothermal IP series consists of:



Acknowledgments

The author is grateful to the many industry, government, research, and legal experts who contributed their time and perspectives through interviews, workshops, and discussions conducted as part of this research. Particular thanks are due to Terra Rogers and Jenna Hill of Clean Air Task Force (CATF), and Peter Massie and Emily Smejkal of the Cascade Institute, for their guidance, thoughtful input, and support throughout the project. Their contributions, together with the insights and expertise shared by interviewees and workshop participants, were invaluable in shaping the analysis and recommendations presented in this report.

Institutional partners



CLEAN AIR
TASK FORCE



Author

Laura K. Mueller is a Legal Fellow at Clean Air Task Force (CATF), where her work focuses on legal and institutional frameworks for geothermal development, including intellectual property, data sharing, and corporate governance. A Swiss-qualified attorney with nearly four years of transactional legal experience at a leading Swiss law firm, she holds an LL.M. (Master of Laws) from Columbia Law School and has passed the New York Bar Examination.

Sharing and permissions

© Cascade Institute and Clean Air Task Force 2026. This report is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits use, sharing, adaptation, distribution, and reproduction in any medium or format, provided appropriate credit is given to the original author and source, a link to the license is provided, and any changes made are indicated. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>

Cover: DEEP Earth Energy Production project site in Saskatchewan, Canada. Used with permission of DEEP. This image is not covered by this publication's Creative Commons license.

Suggested citation: Mueller, L. K. (2026). *Designing for Success: How an Effective IP and Data-Sharing Framework Helps Test Centers Unlock Geothermal Innovation*. Clean Air Task Force, in collaboration with Cascade Institute.

This brief:

- ◆ summarizes the main design options available to test center proponents,
- ◆ highlights the trade-offs associated with different approaches,
- ◆ presents key design principles that recur across successful test centers, and
- ◆ provides a modular toolkit of recommendations that organizers can tailor to **their own objectives and circumstances.**

Test centers are a powerful tool for accelerating energy technology innovation, but they can only succeed if the test center's intellectual property (IP) and data-sharing framework creates commercially credible conditions for participation and value creation. While Issue Brief 1 demonstrated the value of test centers as a mechanism for accelerating innovation, this brief turns to the design challenge at the heart of their success: developing an IP and data-sharing framework that attracts participation, protects proprietary technologies, and enables shared learning, and drives outcomes.

There is no single framework that will work for every energy test center. The optimal framework depends on the ultimate goals of the test center, which are influenced by the national legal framework, the governance and ownership structure, the funding model, the characteristics of the technology being tested, and the composition of the participating industry.

Regardless of these differences, every test center must address the same fundamental design questions:

- i. how participants' pre-existing intellectual property and proprietary information are protected,
- ii. who owns foreground IP (innovations generated through test center activities),
- iii. how data should be shared, and
- iv. how public funding influences these arrangements.

Based on the comparative analysis and recommendations in the complete technical report, this brief provides a practical guide to those design decisions.

Although we present this framework in the context of future geothermal test centers, the recurring principles identified across geothermal, subsurface, and analogous energy-sector programs are relevant to energy test centers more broadly. The recommendations are informed by benchmarking across multiple jurisdictions. Although informed by geothermal, subsurface, and analogous energy-sector programs internationally, the report draws particular insight from U.S. Department of Energy-supported initiatives because they provide a broad range of governance models and established information on IP and data-sharing arrangements.

This brief summarizes the principal options available to test center organizers and participants, highlights the trade-offs associated with different approaches, and introduces key design principles that recur across successful test centers, including tiered data sharing, time-bounded confidentiality, and ring-fencing. Its recommendations should be understood as a modular toolkit that organizers can tailor to their own objectives and circumstances. Readers seeking the detailed benchmarking analysis, more detailed IP and data-sharing recommendations, and an in-depth discussion of public-funding implications under the U.S. reference framework should consult the complete technical report.

Framework design considerations

Private firms invest in innovation to gain a competitive advantage, yet the entire energy sector benefits when knowledge generated through R&D contributes to further innovation. An effective intellectual property (IP) and data-sharing framework reconciles these objectives by creating an environment in which participants share enough information to accelerate collective learning while retaining sufficient control over proprietary technologies and know-how to extract commercial opportunities.

A test center's success depends on getting this balance right. A framework that provides insufficient protection for commercially sensitive technologies is unlikely to attract industry participation. Conversely, a framework that is overly restrictive limits the exchange of operational knowledge and reduces the broader value that shared testing is intended to generate.

Balancing these two objectives is particularly important for geothermal. Much of the sector is being driven by venture-backed companies whose competitive advantage lies in proprietary drilling technologies, high-temperature tools, stimulation methods, software, and technical know-how. As a result, geothermal developers (and the investors backing them) are likely to be more sensitive to intellectual property protection than the oil and gas operators that participated in earlier test centers, such as AOSTRA or the Hydraulic Fracturing Test Sites (see Brief 1).

Consequently, a test center is only as valuable as the participation it attracts. Getting the IP and data-sharing framework right is therefore the difference between a test center that attracts the technologies, expertise, and investment needed to accelerate innovation and one that realizes only a fraction of its potential.

Four core questions

Every test center organizer—whether a public agency, host institution, consortium, or other sponsoring entity—must address a range of legal, governance, and operational considerations. At a high level, the principal questions relating to IP and data sharing that must be addressed at this stage can be organized around four core questions:

- ◆ *How to protect what participants bring into the test center?*
- ◆ *Who owns foreground IP, created through testing and subsequent licensing rights?*
- ◆ *What data should be shared, with whom, and when?*
- ◆ *How does the involvement of public funding affect these choices?*

These questions highlight key IP and data-sharing considerations that test center organizers should address early in the design process, but they are not exhaustive. There is no universal template. Rather, the report identifies a set of recurring design questions and recommends a modular framework that can be adapted to different governance structures, funding models, and

legal systems. Developing and implementing the framework for a particular test center may also require consideration of additional issues based on the applicable legal and regulatory framework, technologies involved, and participating organizations. Some principles, such as protecting background IP and allocating foreground IP based on creation, are remarkably consistent across test centers. Others, particularly data-governance arrangements, require greater calibration to the objectives of the test center, the funding model, and the commercial realities of participating organizations. The sections below summarize the recommended approach; the complete technical report explains the legal rationale and implementation options in detail.

(1) Background IP and proprietary information: Protecting what participants bring into the test center

Participants need assurance that joining a test center will not compromise the technologies, information, and know-how that give them a competitive advantage. The framework should therefore protect the full range of proprietary assets that participants bring into the test center. These may include pre-existing intellectual property rights, such as patents and copyrights, as well as trade secrets, confidential know-how, proprietary technical information, commercially sensitive business information, and other non-public information. The precise legal protection applicable to these assets varies by jurisdiction and by the nature of the asset, but the practical objective is the same: participation should neither transfer participants' pre-existing rights nor require unnecessary disclosure or use of commercially sensitive information.

For purposes of the framework, the report refers to pre-existing intellectual property as background IP and to confidential or non-public information requiring protection as proprietary information. These concepts may overlap depending on the applicable legal and contractual framework. The recommended approach is straightforward: *participants retain ownership of their background IP, while participation agreements protect proprietary information through appropriate confidentiality, access, and use restrictions.*

Strong protection for participants' pre-existing assets is a foundation of participation because it gives developers confidence that joining a shared test center will not compromise their core technologies or commercially valuable information. Three design principles support this approach: Several developments are driving accelerated momentum in geothermal:

- ◆ **Clearly identify the scope of protection.** Background IP should be identified, and proprietary information described with sufficient specificity (e.g., in an annex or schedule), to establish the scope of protection.
- ◆ **Grant only limited operational rights.** Any access required to operate the test center should be provided through narrowly defined operational-use licenses for background IP or limited confidentiality and use rights for Proprietary Information, without creating broader rights to use or commercialize either.
- ◆ **Keep proprietary assets outside of public-funding obligations.** Where public funding supports part of the test center, background IP and proprietary information should remain outside of the funded scope wherever possible through clear contractual ring-fencing.

Across the benchmarked programs examined in Brief 1, protecting participants' pre-existing technologies and information was a consistent feature of the applicable frameworks. Where access was necessary for safe and effective operation, rights were generally limited to what was required for that purpose. This reflects a simple commercial reality: developers will only bring

valuable technologies and information into a shared test environment if they are confident that participation will not compromise their ownership, confidentiality, or competitive position.

(2) Foreground IP: Protecting what is created at the test center

Foreground IP is intellectual property generated through test center activities. The report's default recommendation is that ownership follows creation. Each participant owns the IP it creates. Joint ownership arises only where contributions are inseparable for purposes of obtaining or maintaining protection under applicable IP law (patent and copyright laws). In those cases, the parties may enter into a separate agreement governing their respective rights.

Minimizing joint ownership is an important design objective. Although joint ownership can sometimes be unavoidable, it often results in negative commercial impacts, administrative complexity, and uncertainty, and may create barriers to licensing and investment. Wherever possible, test center activities should therefore be structured so that ownership boundaries remain clear.

The benchmarked programs demonstrate that this can be achieved in practice. At the Hydraulic Fracturing Test Sites, collaborative field testing was deliberately structured so participating companies generated data together while largely avoiding creating jointly developed technologies. Companies continued to compete through their proprietary tools, engineering methods, and interpretation techniques, while benefiting from shared testing infrastructure and shared operational learning. This separation reduced the likelihood of joint inventions while preserving strong incentives for participation.

Where joint or laboratory-generated IP cannot be avoided, participation agreements should define commercialization pathways in advance, including licensing arrangements, internal-use rights, and procedures for future exploitation. The objective is not to eliminate collaboration, but to ensure that collaboration does not create adverse commercial outcomes or unnecessary uncertainty over ownership and use rights.

Public funding may also affect ownership of foreground IP. Where inventions arise from publicly funded activities, statutory or contractual requirements may apply depending on the applicable funding program and jurisdiction. In the U.S. reference framework used throughout the technical report, Department of Energy funding may trigger the Bayh–Dole Act and related regulations, which can introduce disclosure and reporting obligations, government-use rights, participant-specific ownership rules, and public-access requirements for the funded scope of work.¹¹ Similar public-research IP regimes exist in several other jurisdictions. The technical report therefore recommends identifying publicly funded activities clearly and allocating ownership and licensing rights accordingly. The broader implications of public funding for test center design are discussed in Section (4).

(3) Data sharing: How, what, and with whom data are shared

Data sharing should be considered alongside IP allocation from the outset. Test centers generate large volumes of sensitive operational and performance data, and the question of

¹¹ Foreground inventions arising within a Department of Energy-funded scope become “subject inventions” under the Bayh–Dole Act. Universities, nonprofits, and small businesses may elect title automatically. Large for-profit entities do not: title remains with the Department of Energy unless the agency grants a patent waiver. Regardless of who owns the invention, the Department of Energy receives a nonexclusive, irrevocable, paid-up government-use license, which is mandatory and cannot be waived, and retains statutory march-in rights. March-in rights do not permit the government to take ownership of an invention or to obtain trade secrets or proprietary know-how; they are limited to compulsory licensing of patent rights on reasonable terms, and the Department of Energy has not exercised them to date.

who may access data is distinct from the question of who owns an invention. While IP rights are governed by established legal principles, parties retain considerable flexibility in structuring ownership, licensing, and commercialization arrangements by contract. The commercial value of many technologies, however, depends not only on IP rights but also on preserving the confidentiality of proprietary know-how and commercially sensitive information. Data sharing therefore plays a complementary role by determining what information participants must disclose, who may access it, and when it may be shared. It relies much more heavily on contractual and operational design to balance confidentiality with collaboration.

Data-sharing governance therefore requires careful decisions concerning who may access what information, under what conditions, and at what stage of the project. Those decisions are inherently context-specific, depending on the objectives of the test center, the funding model, the commercial sensitivities of participants, and the degree of collaboration sought. In balancing these factors, organizers should also consider potential asymmetries between participants, recognizing that organizations may enter the test center with different technical capabilities, commercial leverage, and existing IP portfolios. The chosen approach should support collaboration without creating disproportionate advantages for certain participants.²

To address these considerations, the report recommends a three-tier data architecture:

Tier	What it covers	How it is treated
Protected background data	<p>Data, models, datasets, and other information that embody, incorporate, reveal, or are derived from a participant's background IP or proprietary information, or that participants otherwise designate as confidential under the participation agreement. This includes information owned or controlled before joining the test center, or developed independently outside the scope of test center activities and any publicly funded work that the participant elects to keep confidential.</p> <p>May include datasets, trade secrets, proprietary designs, materials compositions, manufacturing methods, firmware, internal modeling workflows, commercial or financial information which is privileged or confidential, as well as any pre-existing datasets or models contributed solely for safety or integration.</p>	<p>Remains owned by the contributing party. Disclosed, if at all, only under strict confidentiality and only to the site operator or essential technical personnel.</p> <p>Excluded from public-access expectations, unless the participant affirmatively incorporates such data into the scope of publicly supported work or fails to maintain its confidentiality.</p>
Restricted test data	<p>Operational, observational, and performance-related outputs generated at the test center itself. May include, but are not limited to: drilling parameters, image logs, fibre-optic and microseismic measurements, stimulation diagnostics and reservoir response, standardized performance metrics, and the success or failure of tools tested in situ.</p> <p>Captures what happened in the subsurface, not how a participant's tool is engineered. Can be sub-tiered into raw, derived, and performance-level data.</p>	<p>Shared among participants (or select participants, as deemed appropriate), subject to confidentiality. Access and release may be tailored according to the sensitivity of the data, including staged disclosure following an embargo period or continued confidentiality where justified.</p>
Public data	<p>Outputs ultimately released outside the test center: may include sanitized subsurface datasets, aggregated performance results, benchmark curves, and generalized learnings suitable for public repositories or peer-reviewed publications.</p>	<p>Sanitized before release to remove proprietary identifiers and protect background data. The transition from restricted to public occurs only at the end of any embargo period.</p>

² The challenge of balancing confidentiality with appropriate data sharing is not unique to the energy sector. Other fields, including health care research, financial services, and public digital infrastructure, have addressed analogous questions concerning confidentiality, access controls, and data stewardship. Although the commercial dynamics of multi-party energy test centers differ, the standards and practices developed in these sectors may nonetheless provide useful reference points, complementing the lessons drawn from existing subsurface R&D programs. See, e.g., Digital Governance Standards developed by the Digital Governance Council (Canada) (<https://dgc-cgn.org/digital-standards/?srsltid=AfmBOopVsl1n42Epq-YWZa20GgnSFFXaOsiJrSN0-NC-cZWGGI6XsuGUX#standards>).

To ensure consistent application of these categories, data classifications and access rights should be determined by participants in the first instance, in accordance with the participation agreements and applicable data-governance framework. Where classifications or access rights are disputed, a neutral operator or governance committee should provide an independent mechanism for resolving the disagreement, with unresolved disputes escalating through the test center's established governance and contractual dispute-resolution procedures. For example, disputes over data classification could first be considered by a neutral data-access committee before being escalated to the governing board and, if necessary, the contractual dispute-resolution process.

Embargo periods are the principal commercial incentive. Across the benchmarked programs, early access to high-value operational and subsurface data consistently emerged as the key incentive for industry participation. An embargo provides participants with a period of exclusive access to restricted test data before any required public release, giving them an early competitive advantage. At the Hydraulic Fracturing Test Sites, project data was accessible only to consortium members for three years before non-proprietary datasets were released publicly, and participants described that confidentiality window as the reason the cost-share model made commercial sense. During the embargo, access is limited to all participants (or a defined subset of participants, as determined under the test center's participation and data-governance arrangements), and, in publicly funded test centers, to the relevant public funder for oversight purposes. Participants may use the data internally to refine tools, develop models, and improve operational strategies, and any interpretive or derivative outputs they produce remain proprietary and do not form part of the shared dataset.

The structure of the embargo should be calibrated to the objectives of the test center. One possible implementation is a phased access model that gradually broadens access over time. For example:

- ◆ Years zero to one: Access limited to participating organizations, or designated participants, as appropriate for the relevant data category.
- ◆ Years one to two: Controlled access for approved academic researchers, subject to appropriate confidentiality and use restrictions.
- ◆ Years two to three: Publication of research findings and aggregated results.
- ◆ Year three to five, onward: Public release of non-proprietary datasets.

This is intended only as an illustrative example. The appropriate timing of each stage should be calibrated to the objectives of the test center, the commercial sensitivities of participants, and any applicable public-funding requirements. Depending on the innovation objectives, and taking into account applicable jurisdiction and funding arrangements, publication and public release may occur earlier or later.³

(4) Public funding: How government money affects structuring considerations

Public funding may introduce mandatory IP and data obligations. The report uses the U.S. as its reference case. In that context, two principal regimes apply, depending on how government support is provided. Department of Energy financial assistance, including grants, cooperative agreements, and cost-share arrangements, triggers the Bayh-Dole Act and the Department of

³ For example, in Alberta, Canada, drilling, completion, test, and production data are generally confidential for one year before becoming public, whereas Department of Energy Cooperative Research and Development Agreements may protect certain commercially valuable research data from public disclosure for up to five years.

Energy's implementing regulations. Collaboration with a Department of Energy national laboratory, including in-kind contributions such as laboratory personnel, facilities, equipment, or technical services, triggers the Stevenson-Wydler Act and requires the relationship to be structured through a Cooperative Research and Development Agreement (CRADA).⁴ Both regimes can apply in parallel to different aspects of the same activity. Although applicable legislation and contractual arrangements differ across jurisdictions, many public-funding programs impose broadly comparable obligations relating to IP management, data governance, reporting, and public dissemination.

In the U.S. reference model, these regimes impose obligations such as timely disclosure of subject inventions, restrictions on title election for large, for-profit entities, a mandatory government-use license, march-in rights, a U.S. manufacturing requirement for exclusive licenses, and data-management and public-access obligations. Private in-kind contributions such as rigs, tools, or proprietary equipment are treated as cost share rather than laboratory collaboration and do not by themselves trigger Cooperative Research and Development Agreement requirements. Laboratory involvement does, even where no federal cash funding is provided.

]The key principle is scope. Public-funding rules do not govern the entire test center by default. They generally attach through the award recipient, and they generally apply only to the funded or laboratory-supported scope of work, which must then be integrated into the contractual framework used among private participants. Privately funded work that falls outside the Department of Energy-funded scope remains outside Bayh-Dole, even when conducted at the same physical site. The involvement of the same physical well, samples, or datasets does not by itself merge the regimes.

This makes ring-fencing central to the design. Clear separation of scope, personnel, and data flows ensures that publicly funded and privately funded activities remain distinct and makes clear which activities, IP, and data are subject to federal requirements. Our report recommends a short, standardized compliance module that confirms which activities fall under public funding, recites the applicable provisions, clarifies that they apply only to the funded scope, defines the ring-fencing (separate teams, separate tasks, separate data environments), and requires documentation of which outputs are considered inventions or protected information.

How public support is structured also determines how much information ultimately becomes public, and the benchmarked hybrid models diverge sharply. At the Hydraulic Fracturing Test Sites, nearly all operational activity fell within the Department of Energy-funded project scope, so raw datasets became project data subject to a multi-year embargo followed by public release. At the National Carbon Capture Center, developers often paid for access or operated in ring-fenced scopes outside the Department of Energy-funded tasks, and much of the test data never became project data at all: the Department of Energy received aggregated performance summaries while raw developer datasets remained confidential. A hybrid test center can be structured to resemble either, depending on how the award is drawn and what falls inside the funded scope.

By contrast, FORGE reflects a different governance objective. As a publicly funded research facility, it is intended to maximize scientific dissemination through publication and public deposition of all non-proprietary research data in the Geothermal Data Repository, an approach that has generated substantial value for geothermal research. A commercially oriented geothermal test center is likely to place greater emphasis on protecting proprietary operational information and providing participants with meaningful periods of exclusive access to test data.

4 Entering into a Cooperative Research and Development Agreement involves a multi-step federal approval process, including internal laboratory review and Department of Energy oversight, that often takes six to 12 months to complete.

The legal context determines the rules

An IP and data-sharing framework must fit the legal environment in which the test center operates. There is no off-the-shelf solution, and designers should reason through their own objectives and context rather than replicate another country's model.

The report uses U.S. law, specifically Bayh-Dole and the Cooperative Research and Development Agreement framework, as its reference case. That choice reflects the availability of relevant precedents, established funding mechanisms, and operating test centers, and is intended to ground the analysis in a concrete jurisdictional setting rather than to privilege a U.S.-specific outcome. Comparable constraints on IP generation, licensing, and data disclosure commonly attach to publicly supported research and development in other jurisdictions, implemented through different statutory or policy instruments such as national innovation laws, public-research IP regimes, and government-use safeguards.⁵

The transferable part is not the specific legal form. It is the structural levers: scope-based compliance, ring-fencing, and time-bounded confidentiality. These recur wherever public funding, shared infrastructure, and commercially sensitive innovation intersect, and they can be adapted to other national systems with targeted modifications. The core principles of the framework, including the treatment of background and foreground IP, licensing structures, data tiering, and publication review, are not unique to U.S. law and reflect common design challenges in multi-party research environments.

Cross-border participation deserves early attention. Strong international interest in geothermal means the framework must function predictably for foreign participants. The governing law, funding conditions, and resulting IP and data obligations will necessarily depend on the jurisdiction in which the test center is located. Under a U.S.-based model, foreign entities would retain their home-country background IP, while contractual IP and data obligations may be governed by U.S. law to ensure consistency and enforceability. The same overarching principles can be applied in other jurisdictions, subject to the applicable domestic legal framework.

Governance and ownership models

Existing test centers have accelerated technology development under a range of ownership and governance arrangements. Across our comparative analysis of subsurface test centers, host-led structures (in which a single host institution owns or operationally controls the core test infrastructure and has primary responsibility for its operation) emerged as the predominant ownership model (including Utah FORGE, the Hydraulic Fracturing Test Sites, and the National Carbon Capture Center), reflecting the operational demands of early-stage, capital-intensive infrastructure. At the same time, programs have adopted different governance mechanisms,

⁵ See Section 2.1 and note 2 of the technical report. By way of illustration, comparable public-interest constraints on IP, licensing, and data disclosure apply outside the U.S. through national innovation statutes, public-research IP regimes, and government-use safeguards. Examples include France's *Loi n. 99-587 du 12 juillet 1999 sur l'innovation et la recherche*, university IP ownership frameworks in the United Kingdom, Denmark's *Act on Inventions at Public Research Institutions (Act No. 347/1999)*, and Japan's Bayh-Dole-style framework under Article 30 of the *Act on Special Measures Concerning Revitalization of Industry and Innovation in Industrial Activities (1999)*.

including industry technical committees (the Hydraulic Fracturing Test Sites), consortium-based decision-making (the National Offshore Wind Research and Development Consortium), independent advisory boards representing participants (the National Carbon Capture Center), and independent expert boards (AOSTRA) to reflect their objectives, participants, funding structures, and operational needs. See the summary and technical reports for a detailed analysis of the various governance and ownership models.

Beyond the choice of ownership and governance models, organizers must also decide how governance decisions will be made in practice. The report identifies three approaches to board composition and decision making: an industry-member technical committee, an independent expert board, or a hybrid host-led model. An industry-member technical committee places decisions with experts nominated by participating companies, so field-execution choices reflect the judgment of parties with a direct commercial stake (the Hydraulic Fracturing Test Sites). An independent expert board relies on a neutral body with no ties to participating companies, which suits high-risk experimentation and counter-cyclical investment; this is what allowed AOSTRA to fund the Underground Test Facility when industry would not. A hybrid host-led model centers authority with the host while giving sponsors and industry structured advisory pathways (the National Carbon Capture Center).

Incentives and guardrails

An effective IP and data-sharing framework must answer two practical questions: Why should a company participate in a shared test center, and what gives it confidence that participation will not compromise its competitive advantage?

The incentives: Test centers provide access to scarce, high-cost infrastructure and subsurface conditions that individual companies cannot economically replicate on their own. They also provide credible third-party validation of technology performance, generating independent evidence that can support future investment, regulatory engagement, and commercial deployment. Participation enhances credibility through association with leading and reputable research institutions and industry partners and visibility within a growing ecosystem and creates opportunities for future partnerships and collaborations. It also provides early access to high-quality raw operational data that participants can use to refine technologies before their broader release.

The guardrails: These benefits are only realized when access to shared infrastructure is matched with clear governance protocols. Across the benchmarked programs, the most effective frameworks combined:

- ◆ **Robust protection and ring-fencing of background IP and proprietary information**, with specific listing, no implied licenses, and disclosure only under non-disclosure agreements or a limited operational-use license.
- ◆ **Confidentiality and controlled, tiered data access**, so that what is shared reflects subsurface behaviour rather than tool engineering.
- ◆ **Time-bounded embargo periods** that provide participants with an early-access advantage before broader data release.
- ◆ **Publication review**, allowing removal of proprietary information and patentable subject matter. Raw data and interpretation models are never publishable; performance-level data are publishable after embargo and participant review.

- ◆ **Restrictions on collaborative design work in the field**, to prevent accidental joint inventorship or joint authorship.
- ◆ **Defined licensing rules**, under which participants either receive no rights to other participants' technology, or receive an internal research license for interpretation purposes plus a first right to negotiate commercial licenses to jointly owned or laboratory-owned inventions.

Three principles tie the guardrails together:

- 1. Protect proprietary technology unequivocally.**
- 2. Structure data rights distinctly from IP creation, ownership, and protection.**
- 3. Make public-funding obligations attach only to the funded scope.**

When these principles are reflected in clear contractual arrangements, participation becomes commercially attractive while preserving the knowledge-sharing that gives a test center its broader value.

Recommendations as a toolkit, not a template

There is no universal template, but there is a shared set of questions and a modular toolkit of answers. The framework recommended in the report is deliberately configurable: operators, funders, and participants tailor the modules to their governance structure, funding source, and stage of development. The table below summarizes how the principal elements differ between a fully private or philanthropic test center and a hybrid one that incorporates public support. Because most geothermal test centers are likely to combine private and public funding, the framework is drafted to operate under both.

Element	Fully private or philanthropic	Hybrid (including public support)
Background IP and proprietary information	Full contractual protection; participants retain full ownership of background IP and robust protection of Proprietary Information; no disclosure required except to the operator for site safety.	Same protection. Public funding gives the funder no claim; operator access is for safety and integration purposes only.
Foreground IP	Ownership follows creation under contract, no government rights, fully negotiable.	Local law subject-invention rules apply within the funded scope. <i>U.S. jurisdiction:</i> patent waivers required for large for-profits; government-use license and march-in rights attach there.
Licensing	Fully customizable, exclusive rights freely negotiable and determined by agreement among participants.	Subject to applicable public funding conditions for funded inventions and collaborations. <i>U.S. jurisdiction:</i> Exclusive U.S.-market licenses carry U.S. manufacturing conditions; laboratory-owned Cooperative Research and Development Agreement inventions require funder approval.

Data rights	Multi-tiered architecture governed purely by contract, disclosure is voluntary and calibrated to commercial or philanthropic objectives.	Local public funding restrictions apply. <i>U.S. jurisdiction:</i> Same tiered architecture, with additional data-management and public-access obligations for funded data, and embargo limits as negotiated and approved.
Publication	Optional, full contractual control, long embargoes possible.	Public-access rules generally apply, with carve-outs for proprietary and protected data.
Ring-fencing	Not strictly required, but recommended to distinguish projects, activities, or participants.	Essential. Public-funding obligations generally attach only to the funded scope of work; ring-fencing determines which activities, IP, and data are subject to those obligations.

Governance, IP, and data-sharing frameworks should be addressed early, meaning during feasibility studies, requests for proposals, memoranda of understanding, and other planning stages, rather than as a downstream legal exercise. Early engagement with prospective industry participants, technology developers, investors, public funders, and other stakeholders can identify shared priorities, commercial sensitivities, and potential areas of conflict before they become barriers to participation. It also helps organizers understand which protections, incentives, and governance arrangements are needed to attract participation, allowing the framework to be shaped around the practical needs of future participants. While participation agreements should apply consistently to all participants, equal contractual rights do not necessarily produce equal practical outcomes. Early engagement therefore allows organizers to account for differences in participants' technical capabilities, commercial objectives, and existing positions when calibrating governance arrangements.

The framework presented here focuses on IP and data-sharing arrangements that can help enable and structure participation in a collaborative test center by addressing concerns identified through the comparative analysis of IP and data-sharing arrangements applied in previous research and development programs and raised in ongoing stakeholder discussions. It is not intended to be prescriptive and does not purport to provide a comprehensive IP strategy or address every legal and strategic IP consideration that may arise. Broader and more detailed IP considerations will depend on the applicable legal framework, technologies involved, participants, and commercial objectives and should be addressed with appropriate IP expertise.

Successful test centers also depend on complementary legal and commercial considerations that fall outside the scope of this brief, including land access and the value of leaseholds in well-characterized locations, water rights, reservoir ownership, liability allocation, insurance, and permitting. These must be developed in parallel.

Readers seeking the detailed provisions, the benchmarking behind them, and the full discussion of how public funding affects each module should consult the complete technical report. Together with the summary report and Issue Brief 1, these publications are intended to support governments, host institutions, funders, and industry in establishing commercially credible and collaborative geothermal test centers.