CHICAGO QUANTUM EXCHANGE

Barnes & Thornburg

THE QUANTUM LAW NAVIGATOR

Navigating U.S. Policies, Laws, and Regulations to Advance the Quantum Economy

About the Quantum Law Navigator

What is it? The Quantum Law Navigator is a two-part, ten-chapter report that maps the U.S. policy, legal, and regulatory landscape shaping the quantum industry. It provides clear, practical analysis of four cross-cutting challenges—national security, funding, workforce, and supply chain—to help organizations translate complex rules into actionable strategy.

Who should read it? Leaders and practitioners across the quantum ecosystem—including founders, executives, investors, in-house counsel, and researchers—who need to navigate U.S. legal frameworks to accelerate technology development, commercialization, partnerships, and growth.

Who created it? The Chicago Quantum Exchange and Barnes & Thornburg LLP, with support from leading legal and quantum technology sector advisors.

The Chicago Quantum Exchange is an intellectual hub in Illinois, Wisconsin, and Indiana that advances quantum research, builds the future workforce, and drives the quantum economy by connecting leading universities, national labs, and industry partners. The CQE leads two federal grant initiatives driving national impact: the US Economic Development Administration–designated Bloch Quantum Tech Hub, which is focused on scaling regional assets to compete globally in future industries, and a National Science Foundation Regional Innovation Engines (NSF Engines) Development Award aimed at deepening partnerships and strengthening workforce development plans to drive quantum-enabled security.

Barnes & Thornburg LLP is one of the largest law firms in the United States, known for its broad national reach and deep bench of attorneys across key practice areas. With offices spanning major U.S. cities, the firm represents clients ranging from startups to Fortune 500 companies, government entities, and nonprofits. Its work covers corporate law, litigation, intellectual property, labor and employment, real estate, and regulatory matters, with particular strengths in highly regulated industries such as technology, healthcare, life sciences, and energy. With a focus on combining sophisticated legal knowledge with practical, business-oriented advice, Barnes & Thornburg is recognized for its ability to help clients navigate complex legal challenges while advancing their strategic goals.

> The views expressed herein are those of the authors only and do not necessarily reflect the views of Barnes & Thornburg LLP. This publication is intended for informational purposes only and does not constitute and shall not be relied upon as legal advice. Readers are urged to seek their own legal or other professional advice concerning their specific circumstances or needs. No attorney-client relationship is created by the dissemination of this publication.

© 2025 by the Chicago Quantum Exchange. All Rights Reserved.

Quantum Law Navigator is a trademark of the University of Chicago. The Quantum Law Navigator may not be reproduced in whole or in part, in any form (beyond that copying permitted by sections 107 and 108 of the U.S. Copyright law and excerpts by reviews for public press), without written permission from the publisher. For information, contact the Chicago Quantum Exchange (chicagoquantum.org).

Executive Summary

Quantum technologies are reaching commercial utility and, beginning in the next decade, could reshape how we fight disease, run our cities, secure our data, protect the energy grid, guide ships and airplanes, combat fraud, and defend our country. But this transformative potential also complicates the sector's interactions with legal frameworks, leading to layers of laws and regulations that can impede stakeholders' access to global talent, foreign equipment, public funding, and more.

These challenges grow from quantum's long and uncertain development timelines, scientific complexity, and relevance to national security. Scientists and technologists do not always understand the law, and lawmakers and lawyers do not always understand the science. This disconnect could hinder the development of a robust, sustainable US quantum economy by favoring large institutions that can afford legal teams while discouraging smaller, less-resourced institutions and innovators. If left unaddressed, this disparity could lead to concentration in the quantum market, limiting which innovations reach the public. Ultimately, the lack of diffusion through the US economy could cost the nation its global leadership.

To help address this, the Chicago Quantum Exchange partnered with Barnes & Thornburg LLP to develop the Quantum Law Navigator, a report that helps equip universities, startups, established companies, investors, and policymakers with the tools they need to begin to understand the complex intersection of quantum innovation and legal regimes.

The Navigator has two key aims. The first is to serve as a foundation for critical dialogue between the quantum technology and legal communities by laying out the ways in which the quantum sector interacts with the law, identifying pain points, and mapping out opportunities. These conversations will be key to guiding adaptations that lead to responsible, productive growth. The second is to level the playing field by offering an introductory tool for quantum stakeholders of all types, sizes, and means.

HOW TO USE THE QUANTUM LAW NAVIGATOR

The Navigator is divided into two sections corresponding to these aims.

Part I (Chapters 1 and 2) provides the framework for dialogue between the quantum and law sectors. It is about 10 pages. This section lays out the arguments for bridging the quantum-law gap and examines the US policies, laws, and regulations that impact the sector. These laws are presented through the lens of the four core challenges faced by nations building a quantum economy. Many of the policies, laws, and regulations flow from or are related to these core challenges. They are: (1) Safeguarding national security while fostering quantum innovation; (2) Securing adequate funding for quantum innovation; (3) Confronting the shortage of skilled quantum professionals essential for sustained progress; and (4) Mitigating supply chain vulnerabilities.

This section is the recommended starting place for anyone who wants to understand how the law and quantum interact and why better aligning the two will strengthen the US economy and advance US leadership in quantum technology.

Part II (Chapters 3 through 10) is a tool that users should reference as needed, turning to the sections they most need at any given time. It is organized by eight key legal concepts: Intellectual Property (Chapter 3), Export Controls (Chapter 4), Foreign Investment Controls (Chapter 5), America First Trade Policy and Tariffs (Chapter 6), Global Talent and Immigration (Chapter 7), Government Funding (Chapter 8), Venture Capital (Chapter 9), and Managing Financial Risk (Chapter 10). Each chapter begins by highlighting why the area matters to the quantum sector, then digs into compliance and other details before concluding with key considerations to guide strategy. Recent developments and other key points are called out in boxes throughout the chapters.

This section is for the startup company that needs to know where to begin when it comes to venture capital or wonders whether it is too early to file for a patent. It is for the researcher who needs to understand the obligations associated with government funding or whether she should segment data storage now that she has an international student working in her lab. It is for the company struggling to import critical components, the innovators concerned about their confidential assets in the case of bankruptcy, and the quantum employers trying to make sense of visa and immigration requirements. Ultimately, it is for any quantum stakeholder who needs a starting point for understanding specific issues related to laws, regulations, and compliance.

A LIVING DOCUMENT

The Quantum Law Navigator, while relevant for longer term use, reflects U.S. law as of October 17, 2025. The Quantum Law Navigator is intended as a first edition and the start of a larger initiative. This is an important and fast-evolving topic, and there will be more to examine and unpack in the coming months and years. We encourage readers to visit https://chicagoquantum.org/quantum-law-navigator and subscribe to receive updates on the Quantum Law Navigator project. We welcome ideas and feedback. Please reach out to the QLN team at QLN@uchicago.edu.

Foreword

When DeepSeek shocked the global AI community in January 2025, the quantum technology community took notice as well. The little-known Chinese startup company had released an unexpectedly efficient, low-cost chatbot that raised serious questions about the United States's ability to beat China in the race for technological superiority. It also underscored some salient lessons. First, breakthroughs can come from anywhere or anyone. A tiny startup in Indiana might finally build a working quantum repeater and open the door to the quantum internet. Second, we cannot know whether an unexpected innovation will advance the public good, threaten it, or do both, depending on who uses it. We should assume dual-use developments such as quantum-enabled decryption could arrive at any time, even if conventional wisdom says they remain years away.

Interestingly, both of these possibilities demand a similar response, at least in part: we must close the gap between quantum technology and the law, and we must do it soon. Laws and regulations that aim to keep hostile actors from acquiring quantum technology can create barriers to innovation. We can reduce those barriers by helping scientists understand the law and helping lawyers understand the science. We also must ensure the law is ready for the novel scenarios that may accompany the emergence of a powerful new technology. Again, we can best address this by connecting the quantum technology sector with lawyers, lawmakers, and policymakers, and creating channels for open dialogue.

"Bridging these worlds is not easy. Scientists and lawyers operate in different spheres and speak what can feel like different languages. ... [but] we cannot afford to delay conversations about how quantum technologies and the law interact."

Bridging these worlds is not easy. Scientists and lawyers operate in different spheres and speak what can feel like different languages. I admit I would rather focus on protein qubits and entanglement swapping than worry whether a conversation qualifies as a "deemed export." But I do not have a choice; if I want to pursue the international collaborations that drive scientific advancement, I must understand the rules. Fortunately, I work at a large university with access to legal counsel. Not all scientists share this advantage, and that disparity can limit contributions when the sector needs all hands on deck.

Imagine that a promising researcher at a small institution inadvertently violates export control laws and derails work headed toward a breakthrough. Or consider that regulators might make rules governing foreign hiring, investment, and sensitive technology imports so complex that only the largest, richest quantum companies survive. Concentration, as we know, often stifles innovation. And what if that concentration were to extend to end users, with only the largest companies able to adopt the technologies? That would hinder the widespread diffusion that drives economic impact and global competitive advantage. On the flip side, imagine quantum-enabled decryption arriving before protective post-quantum cryptographic (PQC) algorithms are in place—and imagine that the U.S. lacks the legal guardrails to prevent inventors from sharing that innovation widely.

The truth is, we cannot afford to delay conversations about how quantum technologies and the law interact. For this reason, the Chicago Quantum Exchange partnered with Barnes & Thornburg to develop the Quantum Law Navigator, a report that helps equip universities, companies, investors, and policymakers with the tools they need to begin to understand the complex intersection of quantum innovation and legal regimes. Barnes & Thornburg lawyers with deep knowledge in export controls, intellectual property, government grants and contracts, private funding, immigration, and more offer clear explanations of the laws and how they apply to quantum technology.

We launched the Quantum Law Navigator project in April 2025 with a panel discussion at the University of Chicago Law School, and it aligns with the mission that drove the creation of the CQE at UChicago more than eight years ago. That mission focuses on the development of deep partnerships to seed and develop a Midwest quantum ecosystem that will advance quantum research, expand the workforce, and drive economic growth. Since the CQE launched, our cross-sector community has worked together to ensure widespread participation in the national quantum ecosystem by launching a quantum startup accelerator, bringing cross-sector coalitions together through the U.S. Economic Development Administration-designated Bloch Quantum Tech Hub and a National Science Foundation Regional Innovation Engines Development Award, and building programs to scale the future quantum workforce. These efforts strengthen U.S. leadership in quantum technologies by identifying key gaps and galvanizing Midwest assets to address them. The Quantum Law Navigator marks the latest step in that mission by providing critical tools for the quantum technology sector and laying the foundation for scientists, business leaders, lawyers, lawmakers, and others to engage in dialogue that will shape our quantum future.

David Awschalom
Liew Family Professor of Molecular Engineering and Physics at the University of Chicago;
Founding Director of the Chicago Quantum Exchange;
and Senior Scientist at Argonne National Laboratory

November 3, 2025

Table of Contents

EXECUTIVE SUMMARY 2

FOREWORD 4

ACKNOWLEDGEMENTS 8

PART I – CHALLENGES, POLICIES, AND IMPACTS 10

1. BRIDGING THE QUANTUM-LAW GAP 11

1.1. The Promise of Quantum Technologies 11

1.2. Achieving U.S. Leadership in Quantum 12

1.3. Navigating the Policy and Legal Landscape 13

1.4. The Quantum Law Navigator 13

2. FOUR CORE QUANTUM CHALLENGES 14

Challenge 1 | National Security: Safeguarding National Security While Fostering Quantum Innovation 14

Challenge 2 | Funding: Securing Adequate Funding for Quantum Innovation 16

Challenge 3 | Workforce: Confronting the Growing Shortage of Skilled Quantum Professionals Essential for Sustained Progress 18

Challenge 4 | Supply Chain: Mitigating Supply Chain Vulnerabilities 19

PART II – U.S. POLICIES, LAWS AND REGULATIONS 22

3. INTELLECTUAL PROPERTY RIGHTS AND PROTECTIONS 23

3.1. U.S. Intellectual Property Laws and the QIST Sector 24

3.2. Export Controls Considerations for Patent Filing 27

3.3. Intellectual Property and Government Contracts 28

3.4. Intellectual Property and Venture Capital 30

3.5. Key Agreements 31

3.6. Standards and FRAND Licensing 32

4. EXPORT CONTROLS 34

4.1. Export Administration Regulations 34

4.2. Interim Final Rule 37

4.3. International Traffic in Arms Regulations 41

4.4. Foreign Trade Regulations 42

4.5. Office of Foreign Assets Control 42

4.6. Export Control Classification and U.S. Munitions List Categories 43

5. FOREIGN INVESTMENT CONTROLS 45
5.1. Committee on Foreign Investment in the United States (CFIUS) 45
5.2. Reverse CFIUS 47

6. AMERICA FIRST TRADE POLICY AND TARIFFS 52
6.1. America First Trade Policy and Tariffs 52
6.2. Impacts on Stakeholders 53

7. GLOBAL TALENT AND IMMIGRATION 55
7.1. Key U.S. Immigration Laws 55
7.2. U.S. Immigration Options (Nonimmigrant and Immigrant) 56
7.3. U.S. Immigration System Challenges 60

8. GOVERNMENT FUNDING 63
8.1. Key U.S. Statutes that Promote Government Funding of the Quantum Industry 64
8.2. Available Government Funding and Related Programs 64
8.3. Government Contracting Framework for Quantum Procurement: FAR and DFARS 66
8.4. Government Contracts and Assistance Agreements 67
8.5. Information Release Restrictions 68
8.6. Research Security for Quantum R&D 69
8.7. Management of Disposition of Government Property 72
8.8. Required Actions to Protect Government Interests 72
8.9. SBIR and STTR: Government R&D Funding for Small Business 74

9. VENTURE CAPITAL 76
9.1. Corporate Formation Considerations for Quantum Founders 76
9.2. Investment Structure and Securities 80
9.3. Governance and Control Rights 82
9.4. Economic Terms for Investments 87

10. MANAGING FINANCIAL RISK 92
10.1. Managing Financial Risk 92
10.2. Key U.S. Bankruptcy and Similar Laws 93
10.3. Challenges of U.S. Bankruptcy Laws in the Quantum Industry 95

Acknowledgements

CHAIRS

David Awschalom
Liew Family Professor of Molecular Engineering and Physics, University of Chicago;
Senior Scientist, Argonne National Laboratory;
Director, Chicago Quantum Exchange

Kate Waimey Timmerman
Chief Executive Officer of the Chicago Quantum Exchange

EDITORS-IN-CHIEF

Robert W. Karr, Jr.
Partner, Chicago
Quantum Technology Industry Group Co-Chair
Barnes & Thornburg LLP

Becky Beaupre Gillespie
Director of Communications
Chicago Quantum Exchange

ADVISORS

Aziz Huq
Frank and Bernice J. Greenberg Professor of Law
The University of Chicago

Celia Merzbacher
Executive Director,
Quantum Economic Development Consortium

Hannah Parnes
Head of Policy, EeroQ

ADDITIONAL CONTRIBUTORS

Jean-Luc Cambier
Regional Innovation Officer
The Bloch Quantum Tech Hub and the Chicago Quantum Exchange

Andrew Grotto
Research Scholar, Center for International Security and Cooperation; Director, Program on Geopolitics, Technology, and Governance
Stanford University

Lior Strahilevitz
Sidley Austin Professor of Law
The University of Chicago

Thelma Tennant
Assistant Vice President, Corporate Engagement
The University of Chicago

BARNES & THORNBURG LLP

Luis Arandia
Partner, Washington D.C.
Quantum Technology Industry Group
International Trade Law and Regulations

Drew Bader
Associate, New York
Quantum Technology Industry Group
Emerging Companies & Venture Capital

Michael Carrillo
Partner, Chicago
Quantum Technology Industry Group Co-Chair
Intellectual Property

Scott Carter
Associate, Ann Arbor
Quantum Technology Industry Group
Emerging Companies & Venture Capital

Thomas Donovan
Partner, Chicago
Quantum Technology Industry Group
Intellectual Property

Pia Dorn, Ph.D.
European Transaction Specialist, Chicago
Quantum Technology Industry Group

Sophi J. Gorman
Associate, Minneapolis
Quantum Technology Industry Group
Emerging Companies & Venture Capital

BARNES & THORNBURG LLP *continued*

Mark Hagedorn
Partner, Chicago
Quantum Technology Industry Group
Intellectual Property

Mikaela Heck
Associate, Chicago
Quantum Technology Industry Group

Kenneth Kansa
Partner, Chicago
Restructuring & Bankruptcy

***Robert W. Karr, Jr.**
Partner, Chicago
Quantum Technology Industry Co-Chair
Corporate, M&A, Technology, International

***Maggi Lazarus**
Partner, Washington, D.C.
Quantum Technology Industry Group
Federal Relations Vice Chair

***Christine McCarthy**
Partner, Washington D.C.
Quantum Technology Industry Group
Intellectual Property

Matthew J. Michaels
Partner, Los Angeles
Quantum Technology Industry Group
Federal Contracting, Procurement and
National Security Group Co-Chair

Martin Montes
Partner, Chicago
Quantum Technology Industry Group Co-Chair
Government Relations

Joe Morrison
Partner, Ann Arbor and Los Angeles
Quantum Technology Industry Group
Emerging Companies & Venture Capital Chair

Tejas Shah
Partner, Chicago
Quantum Technology Industry Group
Immigration

Timo Rehbock
Partner, Chicago and New York
Quantum Technology Industry Group
European Practice Group Chair, Logistics and
Transportation Chair

***Robert Weiss**
Partner, Chicago
Quantum Technology Industry Group
Information Technology

Clinton Yu
Partner, Washington D.C.
Quantum Technology Industry Group
International Trade Law and Regulations

*indicates member of the editing team

EDITORS

Meredith Fore
Science Writer
Chicago Quantum Exchange

Julie Johnson
Senior Manager, Client Solutions
Barnes & Thornburg LLP

Cory Zwolinski
Senior Trade Specialist
Barnes & Thornburg LLP

PRODUCTION

Cover art: **Nick Wright**

Interior design and layout: **VisuaLingo**

The CQE and Barnes & Thornburg would also like to thank Juliana Wittig, Stephen Clark, Justin Scott, Leigh Ebrom, Alexa Zackasee, Steve Badger, Joshua Brand, Robin Reisdorf, Justin Hofmeister, Jonathan Froemel, Doni Robinson, Tyler Prich, and Diana Leane for their support and production assistance with this report.

PART I
CHALLENGES, POLICIES, AND IMPACTS

1 | Bridging the Quantum - Law Gap

1.1 THE PROMISE OF QUANTUM TECHNOLOGIES

Quantum information science and technology (QIST) harnesses the properties of matter at nature's smallest scales to unlock capabilities far beyond today's classical technologies. Beginning as early as the next decade, these innovations could reach commercial utility and reshape industries, economies, and societies, with the ultimate potential to shift the global balance of power.

Quantum technologies already support very early, highly specialized applications. Quantum sensors, which are beginning to enter the market, enable the detection of minute environmental changes and deliver unprecedented accuracy in navigation, imaging, and measurement, with current and future applications ranging from defense and climate monitoring to early disease detection and GPS-free navigation. Quantum computers, which some predict could reach commercial utility within five to ten years, may solve once intractable optimization, measurement, and cryptographic problems, revolutionizing sectors from pharmaceuticals to finance. Quantum communication technologies, already in experimental use in Illinois, Massachusetts, Tennessee, and elsewhere, may someday offer nearly perfect information security through entanglement-based networks that immediately break when eavesdropped upon, providing resilience in an era of escalating cyber threats. Quantum networks could also amplify quantum sensing and computing innovations by enabling secure, distributed systems for both.

This vast transformative potential sparks dedicated efforts worldwide, with a growing number of countries investing millions or even billions of dollars in comprehensive initiatives aimed at accelerating QIST and securing global leadership. Although the commercialization timeline varies by application—with quantum computing generally recognized as the furthest out—the QIST sector is now at a pivotal point with initial deployment already underway. NASA has begun using quantum sensors to precisely measure gravity, magnetic fields, and other forces aboard the International Space Station, and in 2024 Boeing completed the world's first recorded flight using multiple quantum navigation systems instead of GPS. Quantum computing companies have shifted toward revenue generation; the leading QC companies have road maps toward scalable universal quantum computers, according to McKinsey's June 2025 Quantum Technology Monitor. Expanded commercialization is expected over the next decade, with total quantum economic value creation projected to grow to nearly $1 trillion by 2035 from about $3 billion today, according to a Boston Consulting Group analysis for the CQE. By 2040, we could see widespread economic integration, with quantum technologies transforming entire industries and everyday life.

Realizing these ambitions, however, requires confronting several vexing core challenges—such as building a domestic supply chain, scaling the quantum workforce, and navigating funding constraints—while simultaneously aiding QIST stakeholders as they navigate the evolving thicket of laws and regulations that grow from these challenges. Points of friction are already emerging. Laws that advance national security often stifle quantum innovation, which itself is essential to national security—creating a conflict without an easy answer. Laws will need to adapt to new technological capabilities, too, both in ways that are already apparent and in ways that have yet to surface.

These efforts cannot wait. Governments and institutions must start working now to align legal frameworks with the accelerating quantum technology landscape to ensure the resilience of the quantum economy—and they must do so in a coordinated and even manner.

In the United States, QIST stakeholders arrive at this pivotal juncture with different tools and at different times. They may stumble into their first patent question, run afoul of deemed export rules that prohibit certain discussions with foreign researchers, or encounter a tangle of rules that impede the acquisition of essential components and materials. Large, well-funded research institutions and companies can retain legal teams, but smaller, less-resourced stakeholders often cannot. Compliance remains costly, confusing, and often discouraging for both groups. The Quantum Law Navigator aims to mitigate this potential chilling effect to ensure that it does not threaten the sector's reach across the domestic economy and, in turn, jeopardize the global leadership the United States has sought to build.

Members of the emerging quantum economy need a common language to understand how legal frameworks intersect with their sector, both to ensure the continued development of their innovations and to clear the way for critical dialogue. If stakeholders do not know how to discuss a shared challenge, they will struggle to address it. The same holds for lawyers and policymakers, especially given the inherent complexity of quantum information science, a field few of them fully understand. That knowledge gap slows efforts to evaluate how fast-changing rules on imports, exports, immigration, and more apply to this equally fast-changing technology.

Creating a common language to unite quantum technologists and lawyers matters globally, too. QIST could upend existing scientific paradigms, generate trillions of dollars in economic value, and reshape global influence. That potential has sparked a worldwide race for technological supremacy even as the need for science-first international collaboration continues. This race brings serious risks, including heightened geopolitical tensions that pressure states caught in the middle; uneven development that leaves some countries economically, technologically, and militarily vulnerable; and the opportunity costs of government limitations on international collaboration.

1.2 ACHIEVING U.S. LEADERSHIP IN QUANTUM

Nations around the world have spent an estimated $56.7 billion USD developing quantum technologies, with China widely regarded as the largest spender at $15.3 billion USD, according to 2025 estimates from QURECA, a UK-based quantum workforce and business development company. QURECA estimates quantum spending at $7.91 billion USD by Japan; $7.67 billion by the United States; $5.49 billion USD by the UK; $3.45 billion USD by Germany; $2.14 billion USD by South Korea; and $1.9 billion USD by Canada. Meanwhile, a growing number of countries and regions have adopted formal national strategies to coordinate and accelerate their QIST efforts, with the UK announcing their first more than a decade ago.

The United States, which was instrumental in launching the quantum revolution through decades of spending on foundational quantum research in universities and national labs, launched its national strategy in 2018 with the National Quantum Initiative (NQI). The NQI Act established a coordinated federal program to accelerate quantum research and development, channeling significant resources and fostering partnerships among universities, national labs, and a dynamic private sector. Four years later, the CHIPS and Science Act amended the NQI Act, authorizing expanded investments in applications-focused research, workforce development, and critical infrastructure and standards. Individual U.S. states, including Illinois, Colorado, Maryland, and New Mexico, are also fueling QIST growth through appropriations, tax incentives, and other measures.

Alongside these domestic investments, the United States has deepened its international cooperation with allies such as Canada, the United Kingdom, European Union members, Japan, South Korea, India, and Australia to pool resources, harmonize standards, and strengthen supply chains. Although difficult, this collaboration is essential to accelerate breakthroughs, ensure interoperability, and address the security and ethical risks of quantum information science and technology. At the same time, strategic rivalry, most notably between the U.S. and China, has driven tighter export controls, curtailed scientific exchange, and threatened to fracture the innovation ecosystem into competing blocs. The drive to quantum leadership forms an integral part of Beijing's broader competition with Washington. China's state-driven approach, exemplified by milestones such as Micius (the world's first quantum communication satellite), leverages vast domestic investment and selective international partnerships with U.S. adversaries such as Russia.

To build a robust quantum economy and avoid ceding quantum leadership, the United States must accelerate domestic QIST progress while carefully managing technology transfer risks that could aid strategic competitors. It must also cultivate a quantum economy that promotes the broad adoption of quantum technologies across sectors and regions. As political scientist Jeffrey Ding notes, scientific breakthroughs constitute only part of technological power; true global success depends on "domestic diffusion"—the ability to integrate new technologies throughout the entire economy. Complexity, long and uncertain deployment timelines, and national security sensitivities set quantum apart from other technologies and can lead to legal and policy hurdles that limit the sector's positive impact on productivity and growth. To address this, the U.S. should focus on pairing research excellence with policies that lower barriers to adoption, expand workforce pipelines, enable

interoperable and secure infrastructure, and ensure that small and medium-sized enterprises, public institutions, and all communities can meaningfully participate in and benefit from quantum advances. One avenue to broad participation is ensuring that QIST stakeholders, regardless of size, are able to understand and comply with relevant laws.

1.3 NAVIGATING THE POLICY AND LEGAL LANDSCAPE

Nations face many of the same hurdles in building a durable quantum economy. Although the list is long, it converges on four core challenges:

1. Safeguarding national security while fostering quantum innovation;
2. Securing adequate funding for quantum innovation;
3. Solving the growing shortage of skilled quantum professionals essential for sustained progress; and
4. Mitigating supply chain vulnerabilities.

Each nation sets its own approach to these challenges based on its own priorities, resources, and geopolitical context, which makes the path to success both highly competitive and rife with trade-offs. How we contend with these challenges will shape not only national outcomes but also the global trajectory of quantum technology.

Viewing quantum policies, laws, and regulations through the lens of these four core challenges offers a useful framework for understanding their purpose and practical application. Legal regimes that govern the QIST sector can be very complex because they serve high-stakes policy goals, and they often fail to fully align with the rapidly changing technological landscape. New technologies, such as artificial intelligence, have caught regulators unprepared and tested existing legal precedent. This is likely to continue as quantum technologies enter the market, raising questions such as how to apply intellectual property protections to quantum algorithms. Technology typically evolves more quickly than the law, and those developing the technologies are not necessarily trained to avoid legal pitfalls or navigate dense compliance requirements.

In addition, aligning legal frameworks across borders is a significant need and challenge. A lack of global harmonization can weaken and disrupt complex supply chains, slow innovation, lead to gaps in information security, and complicate market adoption. The U.S. federal system adds a layer of complexity, too. While the U.S. government continues to provide strategic direction for national quantum initiatives, subnational budget appropriations, state statutes, and municipal ordinances also have significant influence on the quantum innovation landscape. Subnational measures can serve as catalysts for quantum development, but they also introduce an additional regulatory layer. The existence of a patchwork of rules that differ widely in scope, maturity, and enforceability may affect where quantum enterprises choose to locate, allocate capital, attract and retain talent, and manage risk.

1.4 THE QUANTUM LAW NAVIGATOR

The Quantum Law Navigator lowers barriers to full participation in the quantum economy by providing U.S. stakeholders information and logistical considerations as they seek to navigate complex, sector-relevant laws and policies, and to encourage adoption of U.S.-sanctioned quantum standards. This effort begins with a grounded understanding of the distinct policy, legal, and regulatory framework relevant to QIST, which helps industry participants identify compliance issues, reduce transaction costs, and accelerate broad-based yet secure adoption of quantum technology across the economy.

Part I of the Quantum Law Navigator examines the four core challenges, links each to relevant policies, laws, and regulations, explores their impact on stakeholders, and previews navigation strategies.

Part II details navigation strategies in chapters organized by key legal concepts: Intellectual Property (Chapter 3), Export Controls (Chapter 4), Foreign Investment Controls (Chapter 5), America First Trade Policy and Tariffs (Chapter 6), Global Talent and Immigration (Chapter 7), Government Funding (Chapter 8), Venture Capital (Chapter 9), and Managing Financial Risk (Chapter 10).

2 | Four Core Quantum Challenges

The global race to harness quantum science is reshaping the landscape of technological competition and national power. As governments strive to transform quantum potential into real-world advantage, they confront a shared set of formidable challenges. These challenges will ultimately determine the contours of global leadership, influence, and cooperation in the quantum era, as well as when, or even whether, we realize the sector's true technological and economic potential.

Though diverse, these challenges converge on four critical themes: (1) national security dilemmas that arise from quantum's dual-use capabilities (i.e., military and civilian), which both empower and threaten; (2) the immense financial commitments required to develop, scale, and sustain quantum technologies; (3) a persistent shortage of highly skilled talent needed to advance, implement, and secure QIST; and (4) vulnerabilities in global supply chains that expose nations to risks from dependence on foreign sources for essential components and raw materials.

Many stakeholders in the U.S. quantum ecosystem have already faced these challenges to some degree, for example by enduring lengthy hiring processes for specialized talent, struggling to secure essential and often scarce components, or grappling with the intricate and evolving rules that govern access to public funding. The difficulty of finding reliable resources and guidance on the complex web of laws and regulations applicable to the industry only serves to exacerbate these struggles. In addition to these four challenges, stakeholders must grapple with the patchwork system of laws, both among countries and, in the US, among states; the need to prepare for future adversarial use; and questions surrounding responsible development—all issues rife for exploration in future iterations of the Navigator.

Policy choices that address these challenges reflect each nation's industrial base, research ecosystem, fiscal capacity, and geopolitical posture. And choices that leaders make in response to one challenge can impact others. For example, actions that strengthen security can dampen international collaboration. Incentives to speed commercialization may widen regional or sectoral gaps. Efforts to set global standards can erode national leverage. Difficult trade-offs will define the path forward, and strategic judgment will matter as much as technological breakthroughs.

This chapter aims to serve as a general roadmap for stakeholders at all levels. It highlights the key laws and regulatory frameworks related to each major challenge; explains their practical implications for QIST researchers, companies, investors, and policymakers; discusses ways in which these laws may differ when applied to sensitive technologies such as QIST; and directs readers to relevant chapters within the Quantum Law Navigator.

CHALLENGE 1
Safeguarding National Security While Fostering Quantum Innovation

As the United States builds a competitive quantum economy, it faces one of its most complex challenges: safeguarding national security while keeping the path to quantum innovation open. The U.S. approach emphasizes deep research investment, agile public-private partnerships, and targeted international cooperation alongside robust security measures. These policies operate to protect sensitive technologies and prevent illicit transfers. They also require compliance with overlapping legal regimes that can dampen cross-border collaboration and slow scientific progress.

U.S. law shapes how researchers, startups, and industry partners engage foreign collaborators, source critical components and materials, secure financing, and share and protect data. Proactive compliance is essential. In academia, institutions may require additional review for a co-authored paper, and laboratories may delay a visiting scholar's access. In the private sector, regulators may impose burdensome controls when companies export products or technical data, and authorities may require governmental review when a startup raises capital from foreign investors. Failure to anticipate and comply with applicable rules can be fatal.

Heightened scrutiny of the cross-border movement of goods, capital, information, and talent connected to sensitive quantum technologies creates the most common pressure points. Because national security interests underpin these controls, we address them throughout the Quantum Law Navigator, including in sections applicable to global talent, funding, and supply chains.

Navigating the law: What quantum stakeholders may need to know

Due to U.S. national security interests in quantum, sector stakeholders could confront legal restrictions in the following areas:

- **Patent filing requirements.** When seeking patent protection for quantum technologies, businesses should weigh disclosure risks and government restrictions designed to safeguard sensitive technologies against the requirements of filing jurisdictions. International treaties, such as the Patent Cooperation Treaty (PCT), enable a streamlined path to global protection of inventions by preserving priority and deferring country-by-country decisions. But because export controls may cover quantum innovations, companies would be smart to implement additional compliance safeguards before filing abroad or under the PCT. More specifically, industry participants seeking a patent should determine the export-control status of their product, secure any required foreign filing licenses, assess the risk of secrecy orders, and coordinate with counsel experienced in both patent and export-control law. These steps help to ensure compliance with all applicable laws and protect valuable patent rights worldwide. ***(See Chapter 3, "Intellectual Property Rights and Protections.")***

- **U.S. export regulations.** Export Administration Regulations (EAR) govern the export, reexport, and transfer of "dual-use" items, which are technologies with both civilian and military applications. International Traffic in Arms Regulations (ITAR) control the export of defense-related articles and services, which can include certain quantum technologies specifically designed for military use. For QIST stakeholders, these regulations may require registration or licensing, the implementation of internal compliance programs around risk assessment, training, screening, auditing, and more—including compliance with "deemed export" rules that govern information shared with foreign nationals. ***(See Chapter 4, "Export Controls.")***

- **Foreign investment review.** The Committee on Foreign Investment in the United States (CFIUS), an interagency body, reviews and, when needed, blocks or mitigates foreign investments in U.S. companies that develop or possess critical technologies, including those in the quantum sector. Companies seeking foreign investors must track investors and partners, report certain deals to CFIUS, and ensure their products comply with export controls. They also may need to restrict access to sensitive information. These requirements increase legal and administrative costs and also influence decisions about where to build, whom to partner with, and how to secure operations. This process can build investor trust, but it takes time and resources. As a result, some companies have shifted from overseas partnerships to U.S.-based collaborations. ***(See Chapter 5, "Foreign Investment Controls.")***

- **"Reverse" foreign investment review.** The U.S. Outbound Investment Program, a U.S. Treasury initiative effective January 2025 (often called "Reverse CFIUS"), screens outbound investments by U.S. persons involving specified national security technologies, including semiconductors, microelectronics, and quantum technologies, in countries of concern, including China. This screening places additional constraints on investors in companies in the quantum sector and can exacerbate inequalities by favoring stakeholders who know how to navigate the rules, enabling them to unlock government customers, attract blue chip investors, and mitigate risks. ***(See Chapter 5, "Foreign Investment Controls.")***

- **The America First Trade Policy and tariffs.** The America First Trade Policy, renewed in 2025, imposes tariffs to strengthen U.S. technological leadership and national security, with the aim of reshoring manufacturing and reducing reliance on foreign suppliers. Tariffs on components essential to quantum, like ultra-pure metals, precision optics, and advanced electronics can result in higher costs, potential supply chain disruptions, and increased compliance burdens for quantum manufacturers, whether startups or more established companies, and research labs. Although these measures aim to protect intellectual property and secure domestic supply chains, they may also make it harder for quantum companies to source alternatives and manage rising costs. For example, quantum computing firms now pay higher import duties on specialized cryogenic equipment and high-frequency microwave components that are critical for quantum processors, which results in increased production expenses, longer lead times, and the need to identify new suppliers. ***(See Chapter 6, "America First Trade Policy and Tariffs.")***

- **Immigration rules.** The Immigration and Nationality Act (INA) is the foundational body of law that governs immigration and citizenship in the United States. It establishes a framework for all visa categories, permanent residency, and naturalization. To attract and retain foreign talent, quantum stakeholders must track changing immigration measures, maintain strong records, build flexible strategies, coordinate across departments, educate human resources staff, and support international employees. ***(See Chapter 7, "Global Talent and Immigration."***)

- **Buy American Act restrictions.** Companies that develop, manufacture, or supply quantum technologies and seek U.S. government funding or contracts must ensure their products meet strict U.S. domestic content requirements under the Buy American Act. This obligation requires planning supply chains and documentation accordingly and preparing to seek waivers if compliance is not feasible. Meeting these requirements is essential for eligibility and competitiveness in federally funded quantum projects. ***(See Chapter 8, "Government Funding.")***

- **Post-quantum cryptography requirements.** The National Institute of Standards and Technology (NIST) has mandated post-quantum cryptography (PQC) measures that apply to U.S. federal agencies and their contractors. NIST also recommends these measures for any organization concerned with long-term data security, including critical infrastructure and supply chain vendors. ***(To learn more about PQC standards, visit https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.)***

CHALLENGE 2
Securing Adequate Funding for Quantum Innovation

The United States faces distinctive pressures as it secures adequate, sustained funding for quantum research, startups, large-scale infrastructure, and the development of practical applications.

First, delivering fault-tolerant quantum computers, national quantum networks, and advanced sensing systems demands patient, long-horizon capital that exceeds typical venture timelines. Quantum technology depends on specialized equipment, top talent, and intensive research and development, all of which drive heavy up-front investment with uncertain payoff timelines. Creating a utility-scale quantum computer will require multiple breakthroughs across error correction, algorithm development, and physical hardware. No one can know which company or architecture will succeed first. Companies are developing more than half a dozen architectures, including superconducting (Google and IBM), photonic (Xanadu and PsiQuantum), neutral atoms (QuEra and Infleqtion), trapped ions (Quantinuum and IonQ), electrons on helium (primarily EeroQ), and quantum dots (Intel and Diraq).

Second, fragmentation across agencies, regions, and programs creates duplication and leaves gaps, especially at Technology Readiness Levels 4–7, where demonstrations, pilot deployments, and scale-up are most capital-intensive. Third, the United States must balance the benefits of openness with security concerns and supply chain resilience to preserve leadership while protecting critical capabilities.

These pressures ripple across the quantum ecosystem and have sparked serious strategic initiatives by the U.S. government, the private sector, and academic and research institutions.

- **The U.S. government** has taken a proactive, multi-agency approach to secure funding for quantum innovation, primarily through the National Quantum Initiative (NQI) Act of 2018. Subsequent legislation—the fiscal year 2022 National Defense Authorization Act and the CHIPS and Science Act—authorized more than $1.2 billion in federal investment, established the National Quantum Coordination Office, and created major research centers and consortia across the Department of Energy (DOE), the National Science Foundation (NSF), and the National Institute of Standards and Technology (NIST). These agencies fund basic and applied research, infrastructure, and workforce development, and they coordinate efforts to avoid duplication and maximize impact.

In recent years, DOE, NSF, and NIST have received hundreds of millions of dollars annually for quantum research and development, reflecting sustained or increased federal budgets. The government also supports commercialization and technology transfer through programs such as Small Business Innovation Research (SBIR), Other Transaction Authorities (OTAs), and advanced market commitments, which bridge the gap between lab research and commercial deployment. The government acts as an early buyer of quantum systems and provides incentives for domestic supply chain development. (Note: The SBIR and STTR program authorities expired on September 30, 2025, but it is anticipated the authority will be renewed once the government shutdown ends.)

- **The private sector,** including major technology companies such as IBM, Google, and Microsoft, quantum technology companies such as Infleqtion, EeroQ, and PsiQuantum, and suppliers and potential end users, has ramped up investment in quantum technologies, often matching or exceeding public funding. However, quantum remains a high-risk, long-horizon field, and private investment is sensitive to market conditions and perceived return on investment. In 2023, venture capital funding for quantum startups dropped by 50 percent compared with the previous year, reflecting broader technology investment trends.

  To mitigate risk and attract capital, private companies often partner with government agencies and academic institutions, leveraging public grants, joint research projects, and public–private consortia such as the Quantum Economic Development Consortium (QED-C) and the Chicago Quantum Exchange (CQE). These collaborations share costs, expand access to talent, and accelerate innovation. The private sector also advocates for government policies that support supply chain resilience, workforce development, and early-stage market creation.

- **Universities and national labs** drive quantum innovation, conduct foundational research, and train the next generation of quantum scientists and engineers. They also develop the workforce, modernize curricula, and broaden the talent pipeline, which remains constrained. This sector relies heavily on federal grants from DOE, NSF, NIST, the Department of Defense (DOD), and the National Institutes of Health (NIH). It increasingly pursues state and local grants, philanthropic support, and private-sector partnerships to supplement federal funding. Academic institutions also participate in large-scale research centers established by the NQI Act (specifically, the DOE National Quantum Information Science Research Centers and the NSF Quantum Leap Challenge Institutes) and regional innovation hubs that concentrate resources and expertise.

All three sectors recognize that quantum innovation is inherently collaborative and global. The U.S. government has prioritized international cooperation, entering into bilateral agreements and participating in multinational initiatives to pool resources, share knowledge, and ensure secure supply chains. Academia and industry also engage in cross-border research projects and talent exchanges.

Navigating the law: What quantum stakeholders may need to know

Funding brings obligations, and requirements sometimes become more stringent when quantum technologies are involved. Stakeholders may need to consider several legal issues related to government and private funding.

- **Obligations related to government grants, contracts, and other funding mechanisms.** Federal frameworks governing grants, contracts, and other funding mechanisms may impose stringent requirements for protecting intellectual property, safeguarding classified information, maintaining supply chain integrity, and complying with export control laws. Agencies often require contractors to participate in audits and inspections and to submit proposed publications, presentations, or public communications for review and approval before release to prevent inadvertent disclosure of restricted information. The QIST sector often faces more stringent requirements because sensitive algorithms, cryptographic methods, and hardware designs can raise national security concerns. Government agencies offer support programs, but stakeholders need knowledgeable and well-organized legal advice, and they must stay apprised of changing regulations. ***(See Chapter 8, "Government Funding.")***

- **Obligations related to private investment.** Governance and control rights are core considerations when a startup raises outside capital. Investors often expect a defined level of control over and visibility into the company's operations. Startups must understand the economic terms and the rights and privileges associated with the securities they issue to investors. Federal and state securities laws require strict compliance and emphasize that investors in early-stage or high-growth companies should have the opportunity to become fully informed of all material facts about a prospective investment. Startups need careful legal guidance on compliance, which can include regular filings. ***(See Chapter 9, "Venture Capital.")***

- **Foreign investment review.** CFIUS reviews and, when needed, blocks or mitigates foreign investments in U.S. companies that develop or possess critical technologies, including those in the quantum sector. ***(See Chapter 5, "Foreign Investment Controls"; foreign investment review also addressed in Challenge 1.)***

CHALLENGE 3

Confronting the Growing Shortage of Skilled Quantum Professionals Essential for Sustained Progress

The United States leads the world in quantum technology, but a workforce bottleneck increasingly constrains its momentum—a challenge shared across advanced economies. Demand for interdisciplinary expertise in quantum information science and engineering far outpaces the supply of trained professionals, and universities and industry training programs do not yet produce enough talent to meet that demand. The U.S. government has advanced a coordinated policy, legal, and regulatory agenda that links national strategy for quantum workforce development to regional execution, and states have translated these national priorities into regional capacity by building hubs and talent pipelines that connect universities, community colleges, and employers. Still, policymakers must scale the workforce.

As a result, foreign talent remains essential to the U.S. quantum ecosystem, but immigration frictions, green card backlogs, and lengthy security reviews raise labor costs, slow critical programs, and disproportionately impact smaller, less-resourced institutions.

Large universities and established companies can absorb legal and visa costs, run parallel hiring pipelines abroad to hedge against delays, staff dedicated compliance offices, and build in-house quantum training environments that safeguard scarce quantum hardware. But startup companies and smaller colleges and universities have fewer resources to navigate quantum export controls and visa processes, and they are more likely to lose quantum candidates to better-resourced employers.

Navigating the law: What quantum stakeholders may need to know

Below are two of the primary legal areas stakeholders may need to consider:

- **Immigration and visas:** The United States has long depended on global talent, yet visa and work authorization processes are often slow and uncertain, delaying hires and impeding both research timelines and commercialization.

  - **National laboratories** feel these pressures acutely, as the DOE restrictions on foreign talent narrow candidate pools for specialized hardware positions, extend vacancies, and threaten the continuity of critical facilities.

  - **For companies,** restrictive and unpredictable U.S. visa processes hinder quick hiring and retention. The pathways are frequently capped, lottery-driven, expensive, or otherwise constrained. These challenges most affect startups and small laboratories that lack dedicated legal resources. Employment-based green cards can provide a route to permanence, but long backlogs and per-country limits, particularly for nationals of India and China, slow retention and undermine workforce stability. The weakening bipartisan consensus on immigration has made U.S. immigration policy less stable, resulting in greater uncertainty for companies navigating a complex system. This instability puts U.S. companies at a disadvantage compared to countries with streamlined and stable immigration rules for deep-tech workers. As a result, U.S. companies may lose top talent and may need to form international collaborations or distributed teams, which can dilute expertise within the country.

- **At universities,** international scholars and professionals comprise a large share of graduate students, postdoctoral researchers, and new hires, and they often enter through the F-1 STEM OPT program or visas such as H-1B, O-1, and J-1. Although most research institutions and universities in the United States are not limited by the H-1B visa cap, which mainly affects private employers, they still face challenges related to visa processing times, costs, compliance, and volatile immigration policies. These hurdles can delay, complicate, or otherwise make unaffordable the hiring of international quantum researchers, even when the cap does not apply. In addition, universities may hesitate to admit quantum graduate students, postdocs, or visiting scholars from certain countries if the candidates will work on controlled quantum projects. Visa reviews for sensitive quantum technology can further delay or prevent international student participation in quantum labs. Resource disparities across institutions further magnify these problems in quantum science and technology. Finally, increasing scrutiny of international students entering the United States and proposed regulatory changes to U.S. immigration policy are making the United States a less attractive destination for international students, resulting in a marked decrease in international student enrollment in 2025. ***(See Chapter 7, "Global Talent and Immigration.")***

- **U.S. export regulations** apply to international quantum workers through "deemed exports," which occur when a person releases controlled technologies or data to foreign nationals, even domestically within U.S. labs, through visual inspection, conversations, emails, or practical application of knowledge. QIST stakeholders first must determine whether their technology or data appears on the Commerce Control List, and if so, compliance with deemed export rules will be crucial.

  - **For companies,** these rules limit the roles foreign hires can fill and add compliance costs, which are especially onerous for startups. The compliance costs and the risk of violations discourage hiring non-U.S. persons for sensitive work and can limit a company's collaborations with universities, which typically have many international researchers. Larger firms can better absorb these burdens, spread costs, and maintain multiple hiring pipelines. This dynamic produces a stratified market in which scale and location determine who can compete and deliver at the pace the industry demands. It also pushes trained graduates toward competing countries that offer faster and more predictable immigration options.

  - **Universities** must carefully determine when quantum lab training or collaborative quantum research might cross regulatory lines. This obligation can conflict with the academic mission of openness and global collaboration in quantum science. Navigating the complex regulatory landscape, including the Commerce Control List and International Traffic in Arms Regulations (ITAR) categories, requires technical and circumstance-specific legal expertise that many universities, especially in QIST, do not have. Quantum researchers may inadvertently share restricted quantum knowledge, and compliance offices are often under-resourced compared to those in industry. These gaps can lead to uneven enforcement and significant administrative burdens. ***(See Chapter 4, "Export Controls"; deemed export controls also addressed in Challenge 1.)***

CHALLENGE 4
Mitigating Supply Chain Vulnerabilities

The U.S. quantum industry leads technological innovation. As the sector expands, however, supply chain vulnerabilities undermine progress, resilience, and global competitiveness. The core challenge involves securing scarce inputs, including isotopically pure silicon and germanium, rare earth elements, and highly specialized hardware and manufacturing processes.

Foreign suppliers often dominate these markets, creating choke points across the quantum ecosystem. When a single supplier or country controls a critical component or material, any disruption, whether arising from geopolitical tension, trade restriction, or natural disaster, can cascade through the entire chain. The sector's fragmented structure, which spans academic labs, startups, and multinational corporations with complex ownership and partnership networks, heightens risk. And threat actors can exploit weaknesses among smaller, less secure vendors to compromise larger, more secure organizations.

The United States has mounted a coordinated suite of policies, laws, and regulations to harden critical inputs, protect sensitive technologies, and expand domestic capacity. State governments reinforce federal priorities through tax incentives, grants, and site-readiness programs for suppliers in cryogenics, photonics, and microelectronics. Many states also streamline permitting and deploy clean energy credits to offset the high power demands of cryogenic operations and fabrication facilities. Investments in regional ecosystems are accelerating in Illinois, Wisconsin, and Indiana through the Chicago Quantum Exchange; in Colorado, New Mexico, and Wyoming through Elevate Quantum; in Washington state and Oregon through Northwest Quantum Nexus; and in Maryland, Connecticut, Arizona, Texas, Massachusetts, Ohio, and other states that have invested in shared facilities, incubators, and workforce pipelines.

Despite these national and subnational efforts, stakeholders still need additional investment in domestic supply chains and manufacturing capacity to reduce foreign dependence. This need creates further policy opportunities at both levels of government.

It also means stakeholders must work alongside their chosen counsel to navigate laws that tighten trade and capital flows. This obligation applies to U.S. quantum stakeholders importing components and materials, and, as domestic supply grows, to U.S. companies exporting quantum components.

Navigating the law: What quantum stakeholders may need to know

Stakeholders must be aware of laws that can tighten trade and capital flows, including:

- **The America First Trade Policy and tariffs.** Although policymakers designed these measures to increase domestic manufacturing and reduce reliance on foreign suppliers, tariffs on essential components like ultrapure metals, precision optics, and advanced electronics can drive up costs, disrupt the supply chain, and add compliance burdens, forcing companies to search for new suppliers and lengthening production timelines. ***(See Chapter 6, "America First Trade Policy and Tariffs"; America First Trade Policy also addressed in Challenge 1.)***

- **Federal procurement requirements.** Federal agencies must now conduct thorough supply chain risk assessments for all quantum-related procurements. This requirement changes how agencies plan research, purchase equipment, and select partners. For example, the DOE must verify the origin and security of quantum components, such as dilution refrigerators and control electronics, before using them in research projects. Agencies must also check that software and hardware are free from vulnerabilities, especially when connecting quantum systems to classical networks. ***(See Chapter 8, specifically 8.4 on government contracting; government contract requirements also addressed in Challenge 2.)***

- **Foreign investment review.** The Committee on Foreign Investment in the United States (CFIUS) applies rigorous screening to foreign investments that threaten supply chain integrity. These controls aim to protect intellectual property, preserve technological advantage, and prevent adversaries from exploiting U.S. research and manufacturing infrastructure. Although CFIUS generally does not cover standard imports, it could apply in certain scenarios related to quantum technology. ***(See Chapter 5, "Foreign Investment Controls"; CFIUS review also addressed in Challenge 1.)***

- **Export controls.** U.S. regulations can apply to U.S. companies exporting quantum components to other countries. EAR and ITAR restrict the transfer of cryogenic systems, precision lasers, detectors, high-performance data converters, radio frequency and microwave components, vacuum and optical equipment, and related software or technical data. Companies may need licenses to sell certain products abroad, leading some to create domestic demo centers or to limit sensitive data to the United States. Others implement screening programs and technical safeguards to prevent misuse or unauthorized exports. ***(See Chapter 4, "Export Controls"; export controls also addressed in Challenge 1.)***

- **NIST guidance.** The National Institute of Standards and Technology provides detailed guidance for supply chain risk management, including methodologies to identify, assess, and mitigate risks unique to quantum technologies. These measures collectively shape incentives and expectations for both government and industry.

Navigating the complexities outlined above begins with developing basic knowledge about the relevant laws and regulations, understanding how they interact with the quantum technology sector, and developing a strategy for navigating compliance. The remainder of the Navigator provides the foundation for that learning.

Part II is divided into eight key legal concepts that QIST stakeholders confront most consistently. The chapters explain each of the areas, beginning with an explanation of why it matters to the quantum technology sector and then breaking down the relevant policies, laws, regulations, and standards. When applicable, the chapters call out recent changes to law. Each chapter ends with "key considerations" to help QIST stakeholders develop strategies for navigating that legal area.

PART II
U.S. POLICIES, LAWS AND REGULATIONS

3 | Intellectual Property Rights & Protections

WHY THIS MATTERS FOR THE QUANTUM SECTOR

United States intellectual property law safeguards the quantum industry's innovations, creative works, brands, and proprietary information. IP law transforms fragile, hard-won discoveries into assets that companies can own, license, and enforce, and it supplies the legal and economic infrastructure that moves quantum research from academic laboratories to commercial systems and real-world applications. Well-structured IP strategies enable quantum companies to secure market access, manage complex supply chains, and participate in international collaborations by coordinating compliance with overlapping legal regimes. Investors fund companies that hold enforceable exclusivity over core technologies because it reduces the risks associated with competition and imitation. Researchers and engineers choose environments that protect, recognize, and commercialize their innovations.

QIST also brings extra layers of IP consideration that stakeholders must understand and navigate. Long and uncertain deployment timelines, for instance, can make it hard to know when to file for a patent. National security sensitivities may require quantum technology companies to align IP ownership with control over technical data and operate robust compliance programs to reduce regulatory risk and facilitate cross-border operations. QIST stakeholders who receive U.S. government funding may need to understand special obligations related to ownership, licensing, data and patent rights, disclosure and reporting, and march-in rights, which allow the government, under defined conditions, to grant a compulsory license on a privately owned patent to third parties.

Key takeaways:

- Particularized advice and counsel from experienced legal professionals will almost always be a necessity to assist you in navigating the increasingly complex and ever-changing regulatory landscape of quantum technology innovation.
- Patents play a vital role in protecting quantum hardware, control systems, and device architectures, and they demand precise drafting and strategic timing. Teams are generally best served by coordinating filings with publications to protect novelty while participating in academic discourse. Freedom-to-operate analyses and defensive publications can also help teams avoid infringement and secure key innovations.
- Quantum companies use trade secrets to protect proprietary processes and know-how that competitors cannot easily reverse-engineer. Teams can better maintain secrecy with strong access controls and clear policies, especially during cross-institution collaborations. Companies must also manage confidentiality and invention assignments while respecting local labor laws.
- Accepting government funding for quantum research and operations may affect IP rights by requiring the funding recipient to make specific reporting and elections to retain invention rights or allow the government to "march in" and require the patent holder to grant licenses to other parties.
- Software and data raise additional IP issues, including copyright, database rights, and licensing. Open-source choices can boost adoption, but teams should manage them carefully to protect IP. Cloud delivery and data use policies should generally clarify ownership and address privacy, consent, and cross-border rules.
- Collaboration drives quantum research but can complicate IP ownership. Parties can adopt clear agreements that define rights, responsibilities, and licensing, especially in joint projects, university partnerships, and standards activities.

- **A global IP strategy should target key jurisdictions, ensure compliance with export controls, and support effective branding. Clear IP terms in transactions support investment and reduce legal risks. A proactive, integrated IP approach assists quantum technology companies with turning research into valuable assets, securing their advantage, attracting investment, and navigating a rapidly changing market.**
- **Well-crafted IP agreements mitigate legal risks for QIST stakeholders by specifying permitted uses, allocating responsibilities, and outlining procedures for enforcement and dispute resolution. The intention is to foster collaboration by setting clear terms for contributions, background and foreground IP, publication rights, and revenue sharing, enabling parties to work together while protecting their respective interests. In the absence of such agreements, organizations risk losing valuable rights, encountering infringement or trade secret disputes, or facing challenges in establishing ownership.**
- **As noted throughout this report, working closely with legal counsel familiar with the ever-evolving QIST technological and legal landscape will be a critical component of the approach. While this article attempts to bring to the forefront important factors relevant to the construction of that approach, it should not be viewed as a substitute for the absolute necessity of obtaining legal advice tailored to the unique sets of facts and circumstances.**

3.1 U.S. INTELLECTUAL PROPERTY LAWS AND THE QIST SECTOR

No single intellectual property framework protects the full range of innovations in the quantum industry. But together, these legal tools help quantum companies protect their innovations, maintain a competitive advantage, and support growth by transforming scientific advances into scalable, secure, and competitive businesses. Quantum companies and innovators should work with experienced counsel to integrate these IP protections with thoughtful approaches to publishing, standards development, and regulatory compliance. And they should align IP ownership with control over technical data and operate robust compliance programs. This integrated strategy serves as a core component of long-term success in a rapidly evolving and highly competitive field, not merely a legal formality.

3.1.1 Patents

As quantum technologies rapidly evolve, patents secure exclusive rights to novel, nonobvious, and useful inventions such as quantum algorithms, hardware architectures, and error correction methods. These rights arise under the Patent Act as amended by the Leahy-Smith America Invents Act, which introduced a first-inventor-to-file system, expanded the scope of prior art, and established post-grant review processes before the Patent Trial and Appeal Board. The U.S. Patent and Trademark Office examines and issues patents for quantum inventions, and the Bayh-Dole Act governs the ownership of federally funded quantum research, allowing universities and small businesses to retain title to inventions subject to certain government rights and commercialization obligations.

Timing: Under the patent laws of the U.S. and most other countries, inventors should consider the inherent value of filing a patent application disclosing the subject matter of the invention as soon as is practicable under the circumstances. Otherwise, inventors may forfeit valuable patent rights as most jurisdictions around the world operate on a first-to-file system.

The race to file a patent application, however, brings some risks. A patent application explains how to make and use the invention so that a person skilled in the relevant field could replicate it without undue experimentation. Filing a patent application too soon, based only on theory, may result in an application that lacks sufficient disclosure of the important details necessary to make and use the invention without undue experimentation. Additionally, filing a patent application solely based on theory may risk patent eligibility under 35 U.S.C. § 101, which requires that an invention be a new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof. Thus, patent rights generally do not extend to abstract ideas, laws of nature, or physical phenomena that may arise out of pioneering research and development of quantum technology algorithms, protocols, or software.

Secrecy requirements: Patent applicants should also understand government secrecy requirements that may limit patentability based on the possibility that quantum technology could have significant applications in military and national defense and thus may implicate national security concerns. The United States Patent and Trademark Office (USPTO) reviews all patent applications for national security concerns. But because it lacks the technical or operational expertise to independently assess all potential national security risks, it refers certain patent applications to federal departments and defense agencies with specialized knowledge (e.g., the DOD, DOE, and the NSA) to review whether public disclosure might harm national security. This process can result in a secrecy order that prohibits public disclosure and patent application filing outside the U.S.

Government funding conditions: Accepting government funding for research and operations may also affect IP rights by requiring the funding recipient to make specific reporting and elections to retain invention rights. The funding may grant the government a nonexclusive, nontransferable, irrevocable, paid-up license to practice, or have practiced on its behalf, the patented invention for governmental purposes throughout the world. In other words, the federal agencies are allowed to use patented technology without further payment or permission. The funding may also allow the government to "march in" and require the patent holder to grant licenses to other parties, or allow the government to grant them itself, under certain conditions. Further, the funding may limit the manufacture or use of the inventions to the U.S. absent a waiver. Underscoring the importance of obtaining particularized legal guidance, entities engaging in federally funded research should implement systems to train employees in compliance obligations, track inventions, manage disclosures, and comply with any applicable statutory, contractual, or regulatory obligations.

Geographic considerations: Patent application disclosure and potential government restrictions represent only part of the patenting considerations for a participant in the quantum technology industry. Considerations about where to file affect protection strategy and cost, which are important to the long-term success of businesses. Pursuing patents around the world can extend the global reach of patent rights, but typically involves costs for legal services, governmental fees, and translations. So, a well-defined filing strategy can help maximize protection in a cost-effective manner.

The U.S. and most other countries, including Japan, Germany, China, and France, participate in international and regional patent treaties. Such treaties generally allow an initial patent application to provide priority for filing applications to cover the several jurisdictions covered by the treaty, usually within one year. Another option is to file a Patent Cooperation Treaty (PCT) patent application, which allows inventors to retain priority and pursue patent protection in multiple countries through a single international application. This approach can streamline the patent application process by saving time and deferring costs associated with pursuing patent rights globally.

It is necessary to note special considerations for international patent filings when the subject matter is export-controlled, especially in sensitive fields like quantum technology. Before filing abroad or under the PCT, applicants should assess whether the invention is export-controlled, obtain any required foreign filing licenses, and remain aware of the risk of secrecy orders, all in coordination with legal counsel experienced in both patent and export control law. These steps help to ensure legal compliance and preserve valuable patent rights worldwide.

Issue	Impact on International Patent Filing
Export control laws	May restrict or require licensing for foreign or Patent Cooperation Treaty filings
Foreign filing license	Mandatory before filing abroad if the invention was made in the U.S.
Secrecy orders	Can prohibit foreign filings and public disclosure
Treaty participation	Does not exempt from national security or export control requirements
Quantum technology	Often subject to heightened review and export restrictions

A company's patents are valuable assets for securing investment and maximizing the value of commercial activities. Patents grant their owners the exclusive right to make, use, sell, offer for sale, or import an invention for a set period, typically twenty years from the filing date of the application. These rights can be pivotal for startups and established companies alike, providing a competitive edge, enhancing valuation, fostering innovation, and enabling monetization strategies such as licensing.

By preventing competitors from making or selling a patented invention, companies can secure market share and justify the substantial investments required for related research and development. This exclusivity allows strategic pricing, brand positioning, and the establishment of a strong market presence without the downside of immediate imitation.

While patents confer benefits to their owners, they also present risks when others hold them, with such risks often requiring a careful and individualized legal analysis. If a competitor or third party owns a patent that covers a technology or product a company uses, that company may face allegations of infringement. Such disputes can lead to costly litigation, injunctions, and damages awards, as well as the potential loss of market access. Even the threat of a patent infringement suit can disrupt business operations, divert management attention, and strain financial resources. This challenge is especially acute in industries like quantum technology, where overlapping innovations and a dense patent landscape increase the likelihood of unintentional infringement.

In recognition of these opportunities and threats, companies should consider establishing a comprehensive defensive IP strategy that maximizes the value of owned patents while mitigating risks related to others' patents. Freedom-to-operate analyses and patent landscape studies are essential tools to mitigate risks. By proactively identifying relevant third-party patents and evaluating their scope, companies can design around them, seek licenses, or challenge their validity before launching products. Failure to manage these risks can result in halted projects, delayed product launches, and expensive settlements.

3.1.2 Copyrights

Copyrights provide another form of IP that companies can strategically combine with patents to layer protection. The Copyright Act protects original works of authorship relevant to the quantum industry, such as software code, technical documentation, and educational materials. These rights include the ability to control reproduction, distribution, public performance, display, and the creation of derivative works, subject to limitations like fair use. Copyright protection is particularly important for quantum software and publications, which are foundational to both research and commercialization efforts.

Copyright law protects original works of authorship as soon as an author fixes the work in a tangible form of expression. The creator owns the copyright without requiring registration. A simple notice ("© 2025 Quantum Company, Inc. All rights reserved.") can deter unauthorized use. Software and source code, such as quantum compilers and error correction routines, qualify for copyright protection. The design of simulation environments, such as dashboards, visualizations of qubits or circuits, animations of quantum states, and other creative graphical elements and visualization tools, also receives copyright protection.

Companies should consider adopting a well-defined policy and implement agreements for employees and contractors to ensure that all original or derivative works created by employees or contractors within the scope of their employment or engagement qualify as "work made for hire," and constitute the exclusive property of the company unless otherwise agreed in writing. They also should avoid unwittingly copying copyrighted elements from others' work. A well-crafted employment contract drafted by counsel familiar with the technological area can be instrumental in the preservation of a company's IP rights.

3.1.3 Trademarks

Trademarks are vital for quantum companies that seek to distinguish their products and services in a competitive and emerging market. The Lanham Act provides federal protection for brand names, logos, and other source identifiers, which helps prevent consumer confusion and dilution. The USPTO administers the federal trademark registration system, while common law rights and state statutes offer additional layers of protection for marks used in commerce. These legal tools help quantum businesses build and protect their reputations as the industry matures.

Unlike patents, which protect functional inventions, trademarks protect the source identity of a product or service. Trademarks protect brand identifiers, such as names, logos, slogans, and symbols, that distinguish a company's goods or services from those of others. Thus, trademarks, like patents and copyrights, become valuable strategic assets. A valid trademark allows a business to build and defend its reputation by preventing others from using confusingly similar marks that could mislead consumers.

In the fast-growing and complex field of quantum technology, trademarks play a crucial role in both commercialization and trust-building. As companies race to develop quantum processors, algorithms, software platforms, and cryptographic tools, they should establish a distinctive brand identity to gain market recognition and credibility.

Quantum technology companies often enter partnerships, licensing deals, and investment rounds in which the strength of the brand, anchored by registered trademarks, can enhance valuation. Thus, a strong trademark portfolio may be nearly as important as patents in influencing mergers, acquisitions, or global expansion strategies.

3.1.4 Trade Secrets

Trade secrets are especially significant in the quantum sector, where proprietary algorithms, manufacturing processes, and technical know-how can provide a competitive edge. The Economic Espionage Act criminalizes the theft of trade secrets, and the Defend Trade Secrets Act enables federal civil actions to protect confidential quantum information, offering remedies such as injunctions and damages. State laws, largely harmonized by the Uniform Trade Secrets Act, provide parallel protections, which help ensure that sensitive quantum innovations remain secure as companies collaborate and compete in this rapidly advancing field.

While patents often receive the spotlight for safeguarding innovations, and trademarks serve as the face of the company, trade secrets offer a powerful and often underutilized method for preserving competitive advantage. For quantum technology companies, especially those dealing in advanced hardware, proprietary algorithms, or sensitive manufacturing processes, trade secrets can serve as a vital component of an integrated IP strategy. Properly secured and managed, they can create significant value by protecting confidential knowledge that differentiates the company in the marketplace.

Although the U.S. and many foreign countries have trade secret laws, the scope, strength, and enforcement of those laws vary significantly by country. In the U.S., a trade secret includes any information that derives economic value from not being generally known and that the owner subjects to reasonable efforts to maintain its secrecy. This broad definition covers a wide range of potential assets for a quantum technology company, such as qubit control techniques, calibration methods, manufacturing processes for superconducting chips or ion traps, software optimization methodologies, quantum error correction protocols, and internal datasets.

Unlike patents, trade secrets do not require public disclosure and can theoretically last indefinitely, so long as they remain economically valuable and the owner preserves their secrecy. This distinction is particularly valuable for innovations that are difficult to reverse-engineer or explain in a patent or that might fall into a patent-ineligible subject matter area. For example, certain noise mitigation strategies or fine-tuned control parameters may not be easily patentable but can nonetheless provide a critical performance edge. By maintaining these as trade secrets, companies avoid divulging valuable know-how to competitors, allowing them to continue to capitalize on the information internally.

3.2 EXPORT CONTROLS CONSIDERATIONS FOR PATENT FILING

There are special considerations for international patent filings when the subject matter is export-controlled (see Chapter 4 “Export Controls”), especially in sensitive fields like quantum technology. The following discusses why and how export controls intersect with international patent strategy.

- **Export control laws apply to patent filings.** In the U.S., as in many other jurisdictions, export control laws regulate the export of technical data, including information disclosed in patent applications. Filing a patent application in a foreign country or with an international authority, such as under the Patent Cooperation Treaty (PCT), constitutes an export of the invention’s technical information. When an invention involves technology controlled for national security or other sensitive reasons, which includes certain quantum technologies, the USPTO may require a foreign filing license before the applicant submits an application abroad or through the PCT. Applicants should carefully assess applicable controls and licensing requirements before any foreign filing activity.

- **Foreign filing license requirement.** Under 35 U.S.C. § 184, an inventor must obtain a foreign filing license before filing a patent application in a foreign country or with an international authority when the inventor made the invention in the United States. The USPTO automatically reviews all U.S. patent applications for national security concerns, consulting with other agencies as necessary. Failure to secure a required license may result in loss of patent rights, fines, and potential criminal penalties.

- **Secrecy orders and national security.** When the USPTO, after consulting appropriate defense agencies, determines that public disclosure of an invention would harm national security, it may impose a secrecy order. Such an order bars the applicant from filing corresponding applications in foreign jurisdictions and from disclosing the invention to foreign nationals. It also postpones both publication and issuance of any resulting patent until the order is lifted.

- **International patent treaties and export control.** International agreements such as the Paris Convention and the Patent Cooperation Treaty streamline cross-border patent filings, but they do not supersede national export control regimes. Accordingly, U.S. applicants must comply with U.S. export control and secrecy laws before making any international submissions, including those filed through the PCT system.

- **Special considerations for quantum technologies.** Governments have imposed heightened export controls on quantum technologies in response to their dual-use potential across civilian and military domains. The U.S. and several other jurisdictions have expanded regulatory oversight of quantum computing, quantum encryption, and associated hardware, software, and services, reflecting strategic and national security considerations. These measures affect cross-border collaboration, technology transfer, and commercialization pathways.

Patent applications that disclose controlled quantum technologies, when filed outside the country of origin or that involve foreign inventors or agents, may trigger additional governmental review and authorization requirements. Applicants should carefully coordinate export control compliance and patent prosecution to avoid inadvertent violations and to maintain lawful global protection of quantum innovations.

3.3 INTELLECTUAL PROPERTY AND GOVERNMENT CONTRACTS

Negotiating IP in U.S. government contracts for quantum projects requires protecting IP like proprietary algorithms, pulse schedules, calibration methods, device architectures, and control stacks while addressing the government's statutory rights to access, use, reproduce, and disseminate technical data and software created under the award. These governmental rights arise under the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and program-specific data rights regimes, and may support internal government use, interagency missions, and in some cases broader dissemination. The scope of rights depends on the funding source (private expense, mixed funding, or exclusive government funding) and development pathway.

3.3.1 Examples of government contracts and related IP provisions:

- **FAR-based civilian agency contracts.** Under standard FAR clauses (such as FAR 52.227-14), the government by default receives "unlimited rights" to technical data and software first produced in the performance of the contract, which means it can use, disclose, and allow others to use the IP for any purpose. However, if the contractor incorporates privately funded technology ("background IP"), the contractor can assert "limited rights" (for technical data) or "restricted rights" (for software), which significantly limits the government's ability to share or commercialize the technology outside its own use.

- **DFARS-based Department of Defense contracts.** The DFARS (notably DFARS 252.227-7013 and 252.227-7014) introduce "government purpose rights" for technical data and software developed with mixed funding (both government and private). This framework allows the government to use the IP for government purposes, including sharing with other contractors for government work, for a set period of time (usually five years). After that period, the rights may convert to unlimited. Regarding technology developed exclusively at private expense, the contractor may assert "limited rights" or "restricted rights," and thereby seek to preserve greater control.

- **SBIR/STTR contracts and grants.** Small Business Innovation research (SBIR) and Small Business Technology Transfer (STTR) awards include special data rights provisions (see SBIR Policy Directive and FAR 52.227-20). Data generated under these programs enjoys protection from disclosure outside the government for a minimum of twenty years (the "SBIR data rights period"). During that period, the government may use the data internally but cannot disclose it to third parties except in very limited circumstances. This protection is particularly valuable for quantum startups because it preserves commercialization opportunities while still allowing the government to benefit from the innovation. (Note: The SBIR and STTR program authorities expired on September 30, 2025, but it is anticipated the authority will be renewed once the Government shutdown ends.)

- **Other federal funding instruments.** Cooperative Research and Development Agreements (CRADAs) and Other Transaction Agreements (OTAs) often allow flexible, negotiable IP terms. Under a CRADA, a quantum contractor may collaborate with federal laboratories to develop and move new technologies to market. In such circumstances, the nonfederal partner may negotiate an exclusive or nonexclusive license to any CRADA subject invention that results from the collaborative research. Under an OTA, the parties can negotiate bespoke data rights and IP protection terms tailored to the project's needs.

3.3.2 Other federal funding provisions that may apply to QIST stakeholders

- **Invention disclosure and procedural requirements.** Contractors must implement and operate robust IP compliance systems. Core obligations can include prompt disclosure of subject inventions, timely election of title, patent filing with required government rights statements, accurate marking and identification in deliverables, and final invention reporting at closeout. Contractors are generally required to flow down these obligations to subcontractors. In quantum programs, strict controls are essential because of export controls, potential classification, and the strategic value of early-stage patents. Clear segregation and marking of background technology and proprietary data work to protect private rights and prevent unintended government claims.

- **Government IP rights and performer IP rights.** In procurement contracts, the government does not automatically own contractor-developed IP, including IP developed under the contract. The contractor owns background IP and, if it elects under Bayh-Dole or under the contract, it also generally owns subject inventions. The government receives specific license rights based on funding and negotiated terms. Typical government licenses include the following categories: (1) Unlimited Rights for exclusively government-funded development; (2) Government Purpose Rights for mixed funding during a defined period, then conversion to Unlimited Rights; (3) Limited or Restricted Rights for privately funded development that constrain disclosure and non-internal use; and (4) a paid-up, nonexclusive patent license for subject inventions.

  Accordingly, the performer retains ownership of background IP and ownership of elected subject inventions.

  The performer retains exclusive commercialization rights for privately funded IP and control over third-party licensing outside government use, subject to government licenses. Proper marking, assertions, and segregation of data can help to preserve these rights.

  For quantum deliverables that blend funded and proprietary content, contractors should identify and assert background technology before award, restrict government rights to mission needs, and use tailored licenses or protection periods to prevent premature disclosure of competitive technology. A clear IP strategy generally aligns with program objectives and preserve commercialization pathways for quantum sensing, networking, control stacks, and error-correction technologies.

- **March-in rights.** The Bayh-Dole Act establishes march-in rights that allow the government, under defined conditions, to require a contractor, assignee, or exclusive licensee to grant additional licenses to third parties. Grounds include failure to achieve practical application within a reasonable time, unmet health or safety needs, unmet public use requirements, or noncompliance with domestic manufacturing requirements. Agencies have rarely exercised march-in rights. The authority nevertheless provides a meaningful safeguard. In quantum programs, march-in could become relevant if a contractor does not make a critical government-funded capability available to meet essential mission, public health, or national security needs, such as a quantum timing reference, secure communications module, or precision sensor.

- **Exceptional circumstances and advanced government rights.** Agencies may determine that exceptional circumstances warrant a departure from standard Bayh-Dole allocations to protect the public interest. In such cases, contracts may provide enhanced government rights, including expanded data rights, modified government purpose rights, or, in rare cases, government title to certain inventions. Agencies may use this authority in circumstances such as the following:
    - National security imperatives requiring enhanced control or assured access to quantum capabilities.
    - Foundational or critical infrastructure technologies, such as post-quantum cryptography or secure timing networks, demanding reliable availability and interoperability.
    - Risks of monopolization which could impede access or competition.
    - Integration across multiple platforms requiring broad rights free of third-party licensing constraints.

For defense, intelligence, or critical infrastructure programs, agencies may preemptively adopt enhanced rights to ensure long-term sustainment, security, and interoperability of quantum technologies.

3.4 INTELLECTUAL PROPERTY AND VENTURE CAPITAL

Intellectual property creation and ownership are at the core of all tech companies. Potential investors usually make this a top area of focus when they evaluate whether the company formed correctly and whether it is ready for investment. Even very early-stage investment documents include broad intellectual property ownership representations and warranties that require the company to acknowledge by contract that it owns the relevant intellectual property, so founders and founding teams should treat this as a prime area of focus. Diligently maintaining invention disclosures, assignment records, and chain-of-title documentation preserves IP rights by greatly simplifying patent prosecution, trademark filings, licensing negotiations, and IP due diligence in financing rounds and exit transactions.

From inception, the business would typically look to receive an assignment of all intellectual property conceived by founders, employees, consultants, or advisors. Services and employment agreements rely on intellectual property assignment clauses (also called "IP assignments") as foundational terms. An IP assignment clause may include "work for hire" language under the Copyright Act, which ties ownership to copyrighted work product or developments. Investors also generally expect a "present assignment" of all other intellectual property rights as well. A present assignment confirms that the creator of any intellectual property "hereby assigns" all new intellectual property, including trade secrets, know-how, rights in software, trademarks, and patentable subject matter, to the company.

The business should work with an attorney to confirm that its standard-form services agreements include proper IP assignment language and, more importantly, that agreements presented by third-party service providers, such as software development shops or marketing companies, include such language.

Although companies treat founders differently than other service providers in many respects, they rarely treat founders differently with respect to IP assignment. Generally, founders would be expected to execute Proprietary Information and Inventions Assignment Agreements, or sign onto another document that include a strong and broad IP assignment clause, so that the company owns all relevant intellectual property conceived of or created by a founder in connection with the founder's work for the company, even if that work occurred before the company existed.

It is also important for a company to monitor other engagements that a founder, employee, or service provider may have, because concurrent engagements can create conflicting IP assignment clauses and lead to IP ownership disputes. If a founding team member works for the startup on the side or in addition to a full-time job, the company should carefully review and understand any potential conflicts with the assistance of qualified legal counsel.

3.5 KEY AGREEMENTS

Within U.S. intellectual property law, key agreements play a pivotal role in shaping the creation, ownership, use, protection, and transfer of IP rights. These agreements encompass a range of contracts, such as non-disclosure agreements that safeguard confidential information, employment and independent contractor agreements that determine ownership of work product, joint development and sponsored research agreements that facilitate collaborative innovation, and license agreements that permit use and generate revenue. Collectively, these legal instruments help to establish a reliable framework for managing intangible assets throughout the entire innovation process.

3.5.1 Non-Disclosure (Confidentiality) Agreements

Non-Disclosure Agreements (NDAs) serve as legally binding contracts that protect confidential information shared between parties, particularly during early-stage discussions, technical exchanges, or exploratory collaborations. Their importance cannot be overstated. If parties do not use an NDA, even the simplest event can lead to devastating IP loss. NDAs aim to ensure that parties do not use disclosures made during meetings, demonstrations, or pitch sessions without authorization. Prospective investors and partners frequently request access to proprietary information during due diligence. An NDA with robust non-disclosure protections cannot totally prevent unauthorized disclosures, but it can provide heightened motivation to protect information by making vendors, collaborators, partners, investors, consultants, customers, and other outside entities liable for violations.

3.5.2 Employment Agreements

Employment agreements aim to protect information and innovations by requiring employees to maintain confidentiality with respect to proprietary information, both during and after employment, and by specifying how confidential information must be handled and stored. Such confidentiality terms also play an important role in establishing that a company has taken reasonable measures to maintain the secrecy of valuable company trade secrets.

Employment agreements, particularly for engineers, developers, and other technical employees, typically include terms that establish company ownership of inventions and copyrights by including invention disclosure and assignment requirements, as well as language addressing copyrightable works and derivatives. The agreements may also include post-employment provisions that require the return of all confidential materials and IP-related documentation, as well as competitive restrictions, such as non-solicitation and non-compete clauses (where enforceable), to protect confidential or proprietary information from misuse or unintended disclosure after employment. Such provisions further highlight the ongoing obligation to maintain secrecy post-termination.

3.5.3 Joint Development Agreements

Joint Development Agreements (JDAs) are applicable when two or more parties agree to collaborate on a research or product development effort. In quantum technology, JDAs are common when startups or established companies work with academic institutions, government labs, or industry partners to accelerate innovation. A well-structured JDA can address several key issues relating to IP ownership, including defining pre-existing IP, foreground IP developed during the project, and any jointly created IP, as well as use rights, commercialization and revenue sharing, and confidentiality and publication rights. Parties and their counsel should negotiate and draft JDAs carefully to avoid disputes and ambiguity over IP ownership, future use, and commercialization.

3.5.4 Sponsored Research Agreements

Universities play a central role in quantum technology research and typically address sponsored research through carefully structured agreements that allocate IP rights between the institution and the sponsoring party, which is often a company or government agency. Most universities follow a policy of retaining ownership of inventions developed under sponsored research, particularly when university personnel, students, or facilities are involved. However, sponsors usually receive an option to license exclusively or non-exclusively, or first rights to negotiate licensing terms before other licensees.

3.5.5 IP Licensing Agreements

IP licensing allows one party, the licensee, to use IP owned by another party, the licensor, under specified terms. Licensing can take many forms, including inbound licensing, in which companies license foundational IP from universities or national labs to commercialize academic research; outbound licensing, in which companies license their own IP to original equipment manufacturers, software developers, or end users; and cross-licensing, in which companies provide IP rights to competitors or strategic partners.

These agreements may be exclusive or non-exclusive and typically include royalty payments, milestone obligations, and field-of-use limitations. As a result, licensing can provide a key revenue stream and allow a company to scale market reach without directly manufacturing or distributing products.

3.6 STANDARDS AND FRAND LICENSING

Standards that shape intellectual property in the quantum industry emerge from a mix of U.S. and international Standards Setting Organizations, including the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) through Joint Technical Committee (JTC) 1, the European Telecommunications Standards Institute (ETSI), the International Telecommunication Union's Telecommunication Standardization Sector (ITUT), the Internet Engineering Task Force (IETF), and sectoral consortia. Their Intellectual Property Rights (IPR) policies generally require Fair, Reasonable, and Non-Discriminatory (FRAND) licensing of standard essential patents (SEPs) to secure broad access to core quantum technologies. FRAND commitments typically require participants to disclose essential patents in a timely manner during drafting, to negotiate fair and reasonable terms that reflect the value of the contribution rather than enable hold-up, and to make licenses available to all implementers on a non-discriminatory basis. The scope of essentiality and the availability of injunctions remain jurisdiction-specific and continue to evolve through case law and competition policy.

For quantum communications and cryptography, ETSI's work on QKD and ITUT activities on network and security frameworks intersect with NIST publications, including the FIPS and Special Publication (SP) 800 series, and the NIST post-quantum cryptography standards that define interoperability baselines and inform other licensing in security stacks. IEEE efforts on terminology, control, and benchmarking, along with ISO and IEC work on quantum computing, sensing, and testing, shape data formats, error metrics, and conformance regimes that can trigger SEP disclosures. Some communities prefer royalty-free licensing or patent pledges, and implementers must ensure that FRAND obligations remain compatible with open-source licensing models.

Participation in Standards Setting Organizations (SSOs) enables startups, large firms, universities, and agencies to shape technical norms, anticipate essentiality questions, and align product roadmaps with interoperability requirements. U.S. competition agencies review SSO IPR policies for fairness, and federally funded research may be subject to Bayh-Dole obligations that affect ownership and licensing. As the ecosystem matures, patent pools, interoperability testing, and certification schemes will likely complement SSO policies and reduce transaction costs for quantum deployments.

Key Considerations: IP Strategy and Execution

- **Engage expert counsel and maintain records.** Work with IP counsel fluent in both quantum technology and U.S. law. The right advisors distinguish what is patentable from what you should keep a trade secret, craft claims that withstand scrutiny, and avoid traps that trigger rejections or costly disputes. Although general tips and common pitfalls can be identified in reports such as this, obtaining specific legal guidance tailored to your particular circumstance remains a crucial component to your IP strategy. In parallel, maintain impeccable documentation. Record every invention disclosure, experiment, date, and contributor, whether it is a new ion-trap geometry, a cryogenic packaging method, or a qubit error-mitigation workflow. Signed lab notebooks, version-controlled repositories, and clear authorship logs establish ownership, streamline prosecution, and strengthen your position in negotiations or litigation.

- **Build IP strategy from day one.** Map your IP from day one. Decide which inventions warrant patents, which techniques and datasets you will keep as trade secrets, and which names, logos, and content require trademarks or copyrights. In quantum, that can mean patenting a tunable coupler for superconducting qubits, keeping calibration recipes and pulse-optimization code as trade secrets, and trademarking your control software brand while copyrighting its documentation. Early, deliberate choices close gaps that invite imitators and dilute valuation.

- **Safeguard proprietary know-how.** Lock down confidentiality and IP ownership to protect proprietary know-how. Implement non-disclosure agreements and invention-assignment agreements with employees, contractors, university partners, foundries, and investors. However, robust paperwork alone does not suffice. Consider reinforcing these measures with comprehensive training on handling sensitive information, secure lab practices, and clear procedures for reporting and documenting inventive contributions. It may also be useful to remind teams that even making an offhand remark at a conference about an unfiled qubit-reset method or posting calibration data to a public repository can forfeit protection and compromise valuable intellectual property.

- **Scan technology and IP landscape.** Continuously monitor patents, arXiv preprints, conference proceedings, standards activity, and competitor launches to avoid infringement, support freedom-to-operate, and surface licensing or partnership opportunities. Use scans to flag blocking claims in areas like parametric amplification or QKD key reconciliation, reveal white space such as photonic feedforward control, and identify chances to license quantum networking protocols. Track standards bodies, including ETSI for QKD and ITUT groups on quantum communications, so you can hopefully determine where you will need interoperability.

- **Plan for international property protection.** Early planning is essential when seeking international protection for hardware shipments, cloud deployments, or module sales abroad. Timely filing and careful selection of jurisdictions are crucial, as regulations and costs differ significantly across regions such as Europe, Japan, and China. Use the Patent Cooperation Treaty (PCT) route to preserve your options while you assess market interest in technologies like trapped-ion control stacks or diamond spin sensors. Coordinate your filing schedule with planned publications and demonstrations so public disclosures, such as keynote presentations or arXiv postings, are less likely to inadvertently become prior art against your own applications.

- **Treat IP as a living portfolio for strategic advantage.** Treat IP as a living portfolio, not a one-off shield. As products move from lab to manufacturable systems, regularly audit holdings, prune what no longer adds value, maintain and enforce core assets, and capture new innovations. Continuously convert research into filings—for example, improved cryo-CMOS readout chains, faster qubit reset pulses, or more reliable photon sources—while keeping proprietary calibration datasets and fabrication tolerances as trade secrets. Managed this way, IP can serve as a strategic engine for partnerships, licensing, and market leadership, not merely a defensive hedge.

4 | Export Controls

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Quantum technologies sit at the intersection of breakthrough science and high-stakes national security, making U.S. export controls a central design constraint for the industry—and essential learning for many QIST stakeholders. Failure to comply with export controls can have severe consequences, including enforcement exposure.

U.S. export controls relevant to quantum technologies are found in the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), the Foreign Trade Regulations (FTR), and sanctions administered by the Office of Foreign Assets Control (OFAC). Before exporting quantum technologies to foreign persons, companies and research institutions must evaluate technical specifications and end uses, screen collaborators, customers, and destinations for sanctions and restrictions, and maintain documented controls. Failure to comply with all applicable rules could result in the diversion of sensitive quantum capabilities to adversaries' military or strategic programs and triggers significant civil and criminal penalties.

Key takeaways:

- **Recent policy trends, including expanded end-use/end-user rules, Entity List designations, and tighter controls on enabling technologies, signal a durable era of heightened scrutiny.**
- **Impacts vary but remain pervasive. Startups and established firms must classify products and screen customers without stalling growth; cloud and service providers face location and access-control dilemmas; universities and national labs preserve open research while managing "deemed export" risk; investors confront diligence hurdles; and international collaborators navigate licensing timelines and scope limits. Getting compliance wrong causes lost markets, delays, reputational harm, and enforcement exposure; getting it right accelerates commercialization, reduces partnership risk, and attracts capital.**
- **As quantum capabilities advance and policies evolve, competitive advantage will favor organizations that treat export control compliance as a proactive strategic function, embed it in R&D, product design, hiring, and go-to-market, rather than use it as a final gate.**
- **Proactive governance enables responsible collaboration, resilient supply chains, and faster, compliant deployment of quantum technologies to the partners and markets that benefit most.**

4.1 EXPORT ADMINISTRATION REGULATIONS

4.1.1 Overview

The EAR, administered by the Bureau of Industry and Security (BIS) within the Department of Commerce (DOC), imposes controls on the export, reexport, and transfer of quantum-related technologies, software, and technical data. They apply to most commercial items, including dual-use technologies such as quantum computers, quantum sensors, and quantum encryption devices that can serve both civilian and military purposes, and also to certain quantum-related munitions that have moved from defense control to the Commerce Control List (CCL). Stakeholders, including companies, research institutions, and individual researchers, must determine whether their quantum products or research fall within specific Export Control Classification Numbers (ECCNs) on the CCL. If they do, it could trigger licensing requirements, restrictions, or outright prohibitions depending on the destination country, end user, and end use.

The EAR affects stakeholders in multiple areas, as demonstrated by the examples below:

- **Export licensing.** A U.S. quantum computing company seeking to sell or ship quantum processors, cryogenic cooling systems, or specialized quantum software to a customer in China or Russia will likely need to obtain an export license from BIS. Failure to secure the proper license can result in severe penalties.
- **Deemed exports.** If a U.S. research lab shares controlled quantum technology or source code with a foreign national researcher from a country subject to national security controls (such as China or Iran), even if the researcher works within the United States, the EAR treat the transfer as a "deemed export" and that may require a license.
- **Collaborative research.** Joint research projects with foreign universities or companies trigger restrictions if the collaboration involves sharing controlled quantum technology or data with partners in countries subject to EAR controls.
- **Cloud access.** Providing remote access to quantum computing resources (such as cloud-based quantum computers) to users in embargoed or controlled countries can be prohibited or require a license.
- **Supply chain and component sourcing.** Companies should be aware that their procured quantum products that include controlled U.S.-origin components or technology could be subject to reexport rules, even if the final product is manufactured abroad. Training and creating processes for the procurement people in your organization to understand the different nuances and how to conduct the proper due diligence will be essential.

4.1.2 EAR Definition: Export, Reexport, and Transfer

Under both the EAR and ITAR, the concepts of export, reexport, and transfer apply broadly. They cover not only physical shipments, but also electronic transmissions, releases of technology or technical data to foreign persons (even those located within the U.S.), and changes in end use or end user. As a result, U.S. export controls apply to a wide range of activities that could make sensitive items or information available to unauthorized foreign parties or that require specific licenses or authorizations. To ensure compliance, organizations generally should carefully assess all transactions and interactions involving controlled items, technology, or data to determine whether they require U.S. government authorization.

The scope of "export," "reexport," and "transfer" goes beyond shipping physical items abroad.

Under the EAR, an "export" means the actual shipment or transmission of items subject to the EAR out of the United States in any manner. This includes the physical shipment of goods but also the electronic transmission of software or technology, such as by email or cloud upload. The EAR also treat the demonstration, release, or transfer of controlled technology or source code to a foreign person within the United States as an "export." This "deemed export" means that when a party provides a non-U.S. person with access to controlled technology, U.S. law regulates that access as if the party exported the technology to the person's home country, even if the person is physically present in the United States.

A "reexport" under the EAR means the actual shipment or transmission of items subject to the EAR from one foreign country to another. It also includes the release or transfer of controlled technology or source code to a foreign person outside the United States, sometimes termed a "deemed reexport." For example, if a party ships a U.S.-origin item from France to China or shares controlled technology with a Chinese national in Germany, that party has engaged in a reexport under the EAR. The EAR also cover a transfer by a person outside the United States of registration, control, or ownership of certain spacecraft to a person in, or a national of, any other country.

The EAR further define "transfer (in-country)" as a change in end use or end user of an item subject to the EAR within the same foreign country. For example, if a party ships an item to a company in Country A and then provides it to another company or individual in Country A, the party has engaged in an in-country transfer that may require authorization depending on the circumstances.

4.1.3 Compliance Requirements for Deemed Exports

The concept of a "deemed export" under the EAR has significant implications for U.S. organizations that employ foreign nationals. Unlike a traditional export, which involves physically shipping goods, software, or technology out of the country, a deemed export occurs when controlled technology or source code is released to a foreign national within the United States. The EAR treat such a release as if the technology were exported to the foreign national's home country, even if the information never leaves U.S. soil, meaning that the transfer will receive the same level of scrutiny as it would if it were exported abroad. These rules necessitate a proactive, risk-based approach to compliance that integrates export control considerations into hiring, project management, IT security, and other day-to-day operations.

Under this regulatory framework, justifiably careful organizations remain vigilant about what they share domestically with a "foreign national," which the EAR define to mean any employee, contractor, or visitor who is not a U.S. citizen, lawful permanent resident (green card holder), or otherwise classified as a "protected individual" under U.S. immigration law.

The range of activities that can constitute a deemed export is broad. These activities include providing access to controlled technology or source code through visual inspection (such as reading blueprints or technical specifications), oral exchanges of technical information, hands-on training, and allowing access to electronic files or databases containing controlled information. For example, if an organization gives a foreign national engineer access to proprietary manufacturing process details that the EAR control, the organization may be deemed to have exported that technology to the individual's country of citizenship or permanent residence.

To prevent unauthorized releases of controlled technology to foreign nationals, organizations generally implement robust internal controls in concert with legal counsel competent in the area. These controls typically involve several key compliance steps:

- **Technology classification.** Organizations typically look to determine whether any of their technology, software, or technical data is subject to the EAR and, if so, whether the CCL lists it with an ECCN that triggers deemed export licensing requirements.
- **Employee screening.** Before hiring or assigning foreign nationals to projects involving controlled technology, organizations are tasked with assessing the individual's citizenship and immigration status. Organizations often conduct this assessment in conjunction with the Form I-129 certification process for certain visa categories, which requires employers to certify compliance with export control laws.
- **License determination.** If the technology to which a foreign national will have access requires a license for export to that person's home country, a cautious organization will consider applying for and first receive a deemed export license from BIS before allowing access. The licensing process can be lengthy and may not result in approval, especially for nationals of countries subject to strict U.S. controls.
- **Access controls and technology control plans.** Organizations must establish physical and electronic barriers to ensure that only authorized individuals can access controlled technology. This might include compartmentalizing work areas, restricting access to certain computer systems, marking documents as export controlled, and training staff on compliance obligations.
- **Ongoing monitoring and recordkeeping.** Compliance does not end with the initial license or access decision. Organizational recordkeeping is critical and generally involves the maintenance of compliance activity records, monitoring for changes in employee status or project scope, and working with experienced legal counsel to update their controls as regulations or business operations evolve.

Failure to comply with the deemed export rule can result in severe civil and criminal penalties, including fines, loss of export privileges, and reputational harm. Moreover, the rule can affect an organization's ability to recruit and retain top talent from around the world, as it may limit the roles that foreign nationals can fill or delay their participation in sensitive projects.

4.2 INTERIM FINAL RULE

In September 2024, BIS issued an Interim Final Rule (IFR) that significantly expands export controls on quantum computing and related technologies under the EAR in an effort to balance national security interests with the need for international collaboration and innovation. The rule, which took effect on September 6, 2024, marks a landmark development for the quantum industry and introduces new requirements, exceptions, and compliance obligations that can affect a wide range of stakeholders, from startups and research labs to multinational corporations and investors. Organizations will need to pursue proactive compliance and engagement with regulators to navigate this complex and rapidly evolving landscape.

Most importantly, the rule includes new ECCNs that specifically target quantum computers, related hardware, components, materials, software, and technology. The rule also lays out worldwide licensing requirements, licensing exceptions for trusted partners, deemed export and reexport exclusions, and expanded CFIUS implications. These key aspects are outlined below.

Key Aspects of the Interim Final Rule Effective September 6, 2024

New Export Control Classification Numbers

The Interim Final Rule (IFR) adds new ECCNs to the Commerce Control List to address the rapid evolution of quantum technologies. The new entries focus on quantum computers, including ECCN 4A906, and the full ecosystem that enables them, including specialized hardware, components and subassemblies, enabling materials, system software, and related technology and know-how. By carving out clearer, more granular control categories, the rule seeks to ensure that items with the potential to significantly advance quantum performance do not flow to end uses or end users of national security concern without review.

The new ECCNs capture both finished systems and the critical building blocks that make high-performance quantum computing possible. They include processors and modules designed to implement or scale qubits; cryogenic systems and control electronics necessary to operate quantum devices at ultra-low temperatures; precision timing and measurement tools that enhance coherence or fidelity; and specialized materials and fabrication techniques used to manufacture quantum-grade components. The controls also extend to software that materially improves quantum error correction, qubit control, calibration, or system orchestration, as well as technical data and know-how required to design, produce, or use controlled quantum items.

The policy objective is twofold: first, to prevent the unlicensed transfer of capabilities that could materially enhance foreign military, intelligence, or surveillance applications, and second, to provide exporters with clearer compliance guardrails in a fast-moving field. In practice, the new ECCNs trigger license requirements for specified destinations, end users, and end uses, and they may be accompanied by red flags related to advanced system performance, unusually high qubit counts or fidelity metrics, integration into high-assurance cryptanalytic workflows, or procurement patterns indicative of defense or intelligence programs.

For companies and research institutions, the additions call for heightened diligence across the quantum technology development lifecycle, including research and development, prototyping, collaboration, sales, and support. Exporters should routinely reassess product and technology portfolios against the new ECCNs, update internal classification determinations, evaluate deemed export risks for foreign nationals, and strengthen screening for restricted end users and end uses. Contracts, licensing terms, and data sharing practices may need adjustment to reflect new licensing triggers, technology control plans, and recordkeeping obligations.

While the rule is targeted, its scope is intentionally comprehensive. It reaches not only complete quantum computers but also the enabling components, software, and technology that materially contribute to advancing quantum capabilities. Organizations operating in or adjacent to the quantum ecosystem should promptly review the new ECCNs with their legal counsel, seek formal classifications where needed, and implement compliance controls to manage licensing and disclosure obligations under the updated CCL.

Worldwide Licensing Requirements

The IFR establishes a near-universal licensing framework for quantum-related items rather than relying on country-specific export controls. Whereas prior regimes concentrated on a limited set of destinations, the rule applies licensing requirements for exports, reexports, and in-country transfers of covered quantum hardware, software, and technologies to almost all jurisdictions worldwide. This global approach reflects regulators' view that quantum capabilities, spanning sensing, communications, cryptanalysis, and certain enabling manufacturing tools, pose widespread national security and strategic risks if diverted through third-country hubs.

The rule establishes a destination- and risk-based hierarchy for transfers. Transactions involving countries of concern, particularly those in Country Groups D:1 for national security and D:5 for U.S. arms-embargoed countries, face a presumption of denial. In practice, this means applications involving China, Russia, Iran, and other similarly designated states will generally not receive approval absent compelling, narrowly tailored mitigation. By contrast, transactions to close allies and partners, especially those in Country Groups A:5 and A:6, may be eligible for approval when the end use, end user, and compliance controls demonstrate low diversion risk. But even for allies, approvals are not automatic, and applicants should expect detailed scrutiny of technical parameters, supply chain pathways, and downstream integration.

The rule's scope is deliberately broad. It covers direct exports from the United States, reexports from one foreign country to another, in-country transfers within a single foreign jurisdiction, and deemed exports and deemed reexports involving foreign nationals' access to controlled quantum technology or source code, including within research institutions and multinational corporate labs.

While some license exceptions incorporated in the EAR may remain available in limited circumstances, the rule narrows their applicability for quantum items and often their conditions of use based on destination, end user eligibility, and enhanced recordkeeping. Parties should not assume standard exceptions, such as those for certain strategic trade partners, automatically apply to quantum items without careful verification. The familiar exclusions for publicly available information and fundamental research still matter, but they do not extend to tangible items, proprietary designs, or nonpublic enablement technology used to develop, produce, or use covered systems.

Risk management under the rule hinges on rigorous due diligence. Exporters should consider conducting end-user and end-use screening, including checks against the Entity List, military end user and military end use restrictions, and other sanctions lists, and while concurrently assessing red flags such as unusual purchasing patterns, requests for performance beyond stated civilian needs, or intermediary transshipment through high-risk jurisdictions. Technical capability thresholds, integration with cryptographic or surveillance architectures, and links to military or intelligence programs are likely to drive licensing outcomes.

Operationally, organizations and their counsel should map their product portfolios to determine which quantum items and related software or technology fall under control; evaluate global workflows, including research and development collaboration, cloud access, and remote support that could constitute exports of technology or source code; implement access controls for foreign nationals, including project segregation and need-to-know restrictions; harden contract terms with resellers and integrators to prevent diversion, including end-use certificates and audit rights; and maintain robust records to support classification decisions, license applications, post-shipment reporting, and compliance audits.

Finally, companies must consider how the rule interacts with de minimis and foreign direct product principles, which can extend U.S. jurisdiction to certain non-U.S. items that incorporate controlled U.S. content or that manufacturers produce with specified U.S.-origin technology or software. Given the pace of regulatory updates in advanced computing and quantum domains, organizations should consult with counsel to proactively monitor changes and periodically reclassify items. In short, the IFR creates a worldwide, risk-tiered licensing regime for quantum items, tightens controls on countries of concern, and permits case-by-case approvals for trusted partners that can demonstrate strong compliance and low diversion risk.

License Exception for Trusted Partners (IEC)

The IFR introduces a targeted license exception called the Implemented Export Controls (IEC), which streamlines trade in emerging technologies while preserving national security and nonproliferation objectives. Under IEC, qualifying exports, reexports, and in-country transfers of specified quantum-related items may proceed without a BIS license when destined for jurisdictions that have enacted and effectively implemented export controls equivalent to U.S. requirements. By tying license relief to regulatory parity, the exception rewards partners that adopt comparable controls and creates incentives for broader international alignment.

In practice, IEC reduces friction for shipments to a defined set of trusted partners, principally close U.S. allies and economies that participate in major multilateral export control regimes and that have demonstrated enforcement capacity. The Department of Commerce publishes the list of eligible countries and is expected to expand it as additional governments harmonize their rules. The scope of items covered focuses on quantum technologies with national security relevance, such as certain components, subsystems, software, and technology used in quantum computing, sensing, or networking, provided they meet the technical parameters specified in the rule.

Use of IEC is conditional. Exporters must verify that the destination appears on the eligible country list, that the item falls within the IEC scope, and that no separate prohibition applies, such as the Entity List, military end use or end user restrictions, embargoed destinations, or knowledge of prohibited end uses. Standard compliance duties continue to apply, including classification, screening, recordkeeping, and, where required, any reporting or notification associated with the exception. BIS may modify, suspend, or revoke IEC eligibility for specific countries or items based on evolving risk. For companies operating in global quantum supply chains, IEC offers faster and more predictable market access to trusted destinations while maintaining guardrails against diversion and misuse.

Deemed Export and Reexport Exclusions

The IFR acknowledges that quantum research is inherently international, with teams composed of U.S. persons and foreign nationals who collaborate in shared laboratories, universities, startups, and consortia. To preserve legitimate research and workforce mobility while protecting sensitive capabilities, the IFR provides targeted exclusions and general licenses for certain deemed exports and deemed reexports. These mechanisms seek to reduce friction in day-to-day research settings without compromising national security controls.

Specifically, organizations may share some quantum-related items with foreign nationals whose most recent country of citizenship or permanent residency is a designation in Country Group D:1 or D:5, but only under specific conditions. In such circumstances, the IFR does not impose a blanket prohibition on intra-lab or intra-facility sharing, but it treats those interactions as controlled events that raise compliance obligations. In practice, organizations must implement technology control plans, maintain contemporaneous records of access, and submit periodic (often annual) reports that identify the technology or software released, the nationality of recipients, and the scope and duration of access. Qualification for the general licenses depends on robust screening against restricted party lists, adherence to end-use and end-user prohibitions, and immediate cessation of access if red flags arise.

General licenses are standing government authorizations for specific types of transactions, while exclusions are broad exemptions for categories of information or activities from regulations like export controls. The general licenses and exclusions do not provide a free pass. They typically do not cover exports to military or intelligence agencies, or proliferation of end uses or end users, they do not authorize sharing with embargoed or sanctioned parties, and they do not waive other EAR obligations, including rules relating to classification, licensing for higher risk ECCNs, or destination-based controls. Organizations that rely on these provisions should consider documenting eligibility determinations, segregating higher-sensitivity data, and undertaking measures to ensure they release only the minimum necessary technology. The same principles apply for deemed reexports among foreign nationals outside the United States. Eligibility largely depends on the recipients' nationalities, the nature of the technology, and strict compliance with recordkeeping and reporting. In short, the IFR facilitates essential collaboration in quantum research, but it couples that flexibility with structured controls that demand proactive compliance, auditable records, and ongoing monitoring of participants, projects, and technology scope.

Expanded CFIUS Implications

By designating specified quantum technologies as critical technologies, the IFR materially expands the universe of transactions that may trigger mandatory filings with the Committee on Foreign Investment in the United States (CFIUS). Because CFIUS ties its mandatory declaration regime to export control status, quantum items that receive new export control classifications, whether under the EAR or ITAR, can make a U.S. business a TID (Technologies, critical Infrastructure and personal Data) U.S. business and bring both controlling acquisitions and certain non-controlling investments within CFIUS's mandatory scope.

In practical terms, any foreign investment in a U.S. company that designs, tests, manufactures, fabricates, or develops covered quantum technologies may now require a mandatory declaration if an export license would be required to transfer the technology, software, or commodities to the investor, including to its parent or relevant foreign persons in its ownership chain. This can also include minority investments that grant board or observer rights, access to material nonpublic technical information, or involvement in substantive decision-making about critical technology, as well as joint ventures, certain licensing arrangements, and asset deals that convey controlled know-how. Mandatory filing obligations can arise even when the investor is a passive financial sponsor if governance or information rights cross certain CFIUS thresholds.

The IFR heightens due diligence expectations. Parties should consider classifying the target's quantum technology at the outset, determining whether export licenses would be required for the investor's nationalities, and assess whether the target qualifies as a TID U.S. business. Fund structures warrant special scrutiny. While many limited partners are not treated as foreign persons, side letters, advisory committee rights, or negative controls can shift the analysis. Investors from countries likely to require export licenses will likely face increased mandatory filing risk, while excepted investors from excepted foreign states may benefit from limited relief if they meet all criteria.

Deal planning and documentation will need to adapt. Parties may factor in CFIUS risk allocation, mandatory declaration covenants, extended long stop dates, and, where appropriate, mitigation-ready structures that limit access to sensitive technical information and decision making. Boards can anticipate mitigation measures such as access controls, technology segregation, appointment of security officers, third party monitors, or exclusion of certain investor rights. Failure to make a required filing can result in significant penalties and potential unwinding, which underscores the importance of early assessment and an individualized legal analysis by counsel versed in the manner in which CFIUS is applied

Finally, the rule may chill or reshape international collaboration in quantum fields. U.S. companies may prefer investors whose nationality does not trigger export licenses, and syndicates may adjust rights to avoid covered investment features. Licensing, research and development partnerships, and joint ventures will require the same CFIUS and export control attention as equity deals. In short, by elevating quantum technologies to critical technology status, the rule shifts many quantum-related transactions from discretionary review to a regime where mandatory CFIUS engagement is often unavoidable.

4.3 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

4.3.1 Overview

The Directorate of Defense Trade Controls (DDTC) in the Department of State (DOS) administers the ITAR. The ITAR govern the export, temporary import, retransfer, and brokering of defense articles, technical data, and defense services that appear on the U.S. Munitions List (USML), which may include advanced quantum technologies with military applications.

The ITAR impose strict controls on exporting and sharing defense-related quantum technologies, products, software, and technical data that have military applications or are listed on the USML. Stakeholders in the quantum industry, including companies, research institutions, and individual researchers, must recognize the possibility that any quantum technology with potential military or space applications, such as quantum sensors for navigation, quantum encryption for secure communications, or quantum-enhanced radar systems, may be subject to ITAR controls. These controls can significantly limit who can access, work on, or receive such technology, both within the U.S. and abroad.

Examples of ITAR impacts on stakeholders include:

- **Personnel restrictions.** U.S. quantum companies or research labs working on ITAR-controlled quantum sensors or communication systems may not allow foreign nationals, including students, researchers, or employees, to access controlled technology or data without specific U.S. government authorization, even if the work occurs entirely within the United States.
- **Export licensing.** Exporters must obtain a license from the U.S. Department of State before exporting ITAR-controlled quantum hardware, software, or technical data, including quantum navigation systems or quantum cryptography modules, to any foreign country or entity. The Department of State rarely grants licenses for exports to countries subject to arms embargoes or considered adversaries.
- **Collaborative research.** The ITAR place significant restrictions on joint research projects with foreign universities or companies that involve ITAR-controlled quantum technology. U.S. partners must ensure they do not share controlled information with unauthorized foreign collaborators, which limits international scientific collaboration and slows innovation.
- **Publication and conferences.** The ITAR may restrict public presentations or publications that include ITAR-controlled quantum technology, because disseminating technical data to foreign persons, even at international conferences or through online publications, can constitute an export.
- **Supply chain and manufacturing.** U.S. quantum companies must work to ensure they do not expose their supply chains and manufacturing partners, including those abroad, to ITAR-controlled technology without proper authorization, which complicates global sourcing and production strategies.

Overall, ITAR compliance requires quantum industry stakeholders to implement rigorous access controls, conduct thorough screening of personnel and partners, and seek legal guidance before engaging in international activities, to avoid severe civil and criminal penalties and to protect U.S. national security interests.

4.3.2 ITAR Definitions: Export, Reexport, and Transfer

The ITAR provide definitions that are similarly broad to those in the EAR (see Section 4.1).

An "export" under ITAR means sending or taking a defense article out of the United States in any manner and includes transferring registration, control, or ownership to a foreign person. ITAR covers disclosing or transferring technical data to a foreign person, whether in the United States or abroad. An oral or visual disclosure of controlled technical data to a non-U.S. person within the United States counts as an export, which closely parallels the EAR's "deemed export" rule. Additionally, a person exports by performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad, under ITAR.

A “reexport” under ITAR means transferring a defense article or technical data from one foreign country to another foreign country, or transferring technical data or defense services to a foreign person in a third country.

ITAR uses the term “retransfer” to mean the transfer of a defense article or technical data to an end user or for an end use not previously authorized, even within the same country. For example, if a defense article is exported to Company A in Country X, and Company A then provides the article to Company B in Country X, Company A has retransferred the article and may require U.S. government approval.

4.4 FOREIGN TRADE REGULATIONS

The U.S. Census Bureau administers the Foreign Trade Regulations (FTR), and U.S. Customs and Border Protection (USCBP) enforces them. The FTR require exporters, including those in the quantum industry, to file Electronic Export Information (EEI) through the Automated Export System (AES) for most shipments of goods, technology, or software leaving the United States. This reporting obligation applies regardless of whether the export requires a license under the EAR or ITAR. For stakeholders in the quantum sector, the FTR give the U.S. government visibility into the movement of sensitive quantum products and technology, support enforcement of export controls, and enable statistical tracking of trade flows.

Examples of FTR impacts on stakeholders include:

- **Mandatory reporting.** A quantum hardware manufacturer that ships quantum processors, cryogenic cooling systems, or specialized quantum sensors abroad will need to file an EEI in AES and provide details including, but not necessarily limited to, the item description, value, destination, end user, and applicable export control classification number (ECCN or USML category).
- **Compliance with export controls.** Even if a quantum technology export does not require a license, the FTR still mandates reporting, which helps authorities monitor for potential unauthorized or suspicious shipments, especially to high-risk destinations.
- **Penalties for non-compliance.** Authorities can impose significant civil and criminal penalties for failure to file, late filing, or inaccurate reporting, including fines and loss of export privileges, which can disrupt business operations and damage reputations.
- **Facilitating due diligence.** The FTR’s reporting requirements encourage quantum companies to maintain accurate records, verify end users and destinations, and coordinate with freight forwarders and compliance teams to ensure proper documentation and lawful exports.
- **Supporting research and policy.** Data collected under the FTR help the government and industry analyze trends in the export of quantum technologies, informing policy decisions and supporting efforts to maintain U.S. leadership in the field.

4.5 OFFICE OF FOREIGN ASSETS CONTROL

The Office of Foreign Assets Control (OFAC) enforces U.S. economic and trade sanctions that significantly affect stakeholders in the quantum industry, including companies, research institutions, and individual researchers. OFAC prohibits or restricts U.S. persons and entities from transacting, collaborating, or transferring quantum technologies, software, or technical data with sanctioned countries, entities, or individuals. These restrictions cover direct and indirect dealings, including joint research, licensing, investment, and providing cloud-based quantum computing access. Violations can carry severe civil and criminal penalties, including fines and loss of export privileges.

Examples of OFAC impacts on stakeholders include:

- **Prohibited collaborations.** A U.S. quantum computing company may not enter a research partnership or share technology with an entity or individual in a comprehensively sanctioned country (such as Iran, North Korea, or Russia) without a specific OFAC license, even if the collaboration occurs virtually or involves open-source research.
- **Blocked transactions.** If a quantum technology firm identifies a potential customer or investor on OFAC's Specially Designated Nationals (SDN) list, the firm is required to immediately block the transaction and report it to OFAC, regardless of the business opportunity.
- **Cloud access restrictions.** Firms generally may not provide remote access to quantum computing resources or software to users in sanctioned jurisdictions, even if they deliver the service over the internet.
- **Secondary sanctions risk.** Non-U.S. companies that facilitate significant transactions involving U.S.-origin quantum technology with sanctioned parties may face secondary sanctions that restrict access to the U.S. market or financial system.
- **Due diligence and screening.** Quantum industry stakeholders should consider implementing robust compliance programs that screen all customers, partners, and transactions against OFAC's sanctions lists and help to ensure they do not engage in prohibited dealings, even inadvertently.

4.6 EXPORT CONTROL CLASSIFICATION AND U.S. MUNITIONS LIST CATEGORIES

At the heart of compliance for the quantum industry, companies must determine jurisdiction and classify quantum-related items and technology. In September 2024, the Bureau of Industry and Security introduced new Export Control Classification Numbers specifically for quantum technologies, reflecting the growing importance and sensitivity of this sector. (See Key Aspects of the Interim Final Rule Effective September 6, 2024 in Section 4.2) Companies that develop or export quantum computers, quantum communication systems, quantum sensors, or related software should analyze whether their products fall under the Commerce or State regime, after which they are able to classify them under one of the new ECCNs on the Commerce Control List or a category on the U.S. Munitions List.

The new ECCNs cover a range of quantum items, including quantum computers, components, materials, software, and technology, and they address both national security and foreign policy concerns. Many low-risk quantum components may still fall under EAR99, but sensitive quantum technologies, such as high-performance quantum processors, quantum cryptography systems, and quantum-enabled military devices, now more likely fall under these new ECCNs and often require licenses.

Exporters in the quantum sector would also be wise to analyze the destination, end user, and end use of their products. Country-based controls, including comprehensive and targeted embargoes, determine whether a license is required for quantum exports. Screening against government lists helps identify parties that are denied or restricted, which is particularly important given the strategic value of quantum technology. Even where a license might otherwise be needed, the EAR provides license exceptions for defined circumstances, though their conditions remain strict and recordkeeping is essential.

Key Considerations: Export Controls

- **Multiple regulatory environments.** Export controls cross into more than one set of regulations. Organizations must ensure compliance across all of these environments and understand the nuances between them. ITAR and EAR use a different classification list but a very similar definition of "deemed export." It's important to partner with a trade professional who can help navigate these regulatory areas early on in your mapping process.

- **Importance of jurisdiction and classification processes.** The proper classification of your items and technology is one of the most important tasks of any export control program, particularly in the rapidly and ever-changing world of quantum technology. The applicable controls, exclusions, and licensing requirements for your program will all be driven by the proper jurisdiction and classification processes being applied. Developing these processes and the associated recordkeeping are essential components of a successful export compliance program. Remember that these regulations will also apply to intangible items such as technology as well.

- **Know your partners/end users/end uses/staff.** Be aware of the destination, end user, end use of your products/technology, and your staff to avoid unplanned slowdowns, or worse: being caught in an inadvertent violation. Addressing the red flags associated with these areas will help companies stay out of trouble and competitive in this sector. Examples of this would be: an unexpected foreign national working on a controlled program without proper licensing; not knowing that an item is intended for one of the many controlled end uses at the time of startup or, even worse, when it's time to export or transfer the item; or not properly screening a third party involved in a capacity which would require access to controlled technology.

- **Have a licensing strategy.** Identifying and planning for potential scenarios needing licensing from one or more relevant regulatory environments will be essential to a successful export compliance program. They are a necessary part of this process in some cases but being prepared and having the proper people and processes in place can make them less impactful on the overall process versus running into them in the middle of a very important milestone that will bring your progress to a complete stop until the appropriate licensing can be obtained. Don't forget to check for licensing exceptions if your items are in the jurisdiction of the EAR, no exceptions are available for the ITAR, however, they do have specific exemptions that may apply in certain scenarios. Having someone who knows how to make this decision correctly can be invaluable to your business.

- **Prevent violations.** Of course, nobody wants to knowingly or accidentally commit a violation, but these things happen sometimes even to the best compliance programs. Early identification and proper reporting channels demonstrate to regulators a commitment to compliance and can potentially help mitigate any incoming penalties. Additional processes that can help prevent and/or identify issues early in a program are in-depth tailored training for applicable parties involved in these specialized processes and general awareness training if not directly involved. This will help everyone to be on alert for potential violations so they can try to prevent them. Record keeping, a well-documented export compliance audit process, and well-defined compliance roles can also help companies avoid and address potential issues before they turn into violations. These concepts apply across most regulatory environments, and export controls are no different.

- **Flow-down compliance.** Export controls will touch every area of your business. So, finding a partner who can provide an all-in-one solution early on will be very beneficial for organizations looking to build a culture of compliance. Export controls have an expansive regulatory framework that crosses into multiple jurisdictions, so it makes sense there is no one thing that can make a compliance program successful. The message needs to come from the top and work its way through every stakeholder in your organization. Because by the time you are ready to deliver to your customer or engage in a partnership in the quantum environment, you will have exposed every area of your business to some sort of export control process. R&D: they'll develop the item or technology that needs to be classified with their help. Sales: they will begin taking it out to the market after ensuring they know who and where the products/technology will be going and what they will be used for and all the while looking for and clearing potential compliance red flags. Engineering: providing after-sales maintenance, upgrades and other services all the while ensuring they are doing so within the provisions of their licenses or exemptions where applicable.

5 | Foreign Investment Controls

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Foreign investment controls increasingly shape the development and financing of quantum technologies, which policymakers view as critical to national security because these technologies can affect encryption, intelligence, and advanced manufacturing. In the United States, the Committee on Foreign Investment in the United States (CFIUS) reviews inbound deals for risks tied to critical technologies, sensitive data, and critical infrastructure, categories that routinely include quantum hardware, enabling components such as cryogenics, control electronics, and advanced materials, as well as associated IP and data. CFIUS profoundly affects all stakeholders in the quantum industry, often creating significant challenges for startups, investors, academia, and the broader ecosystem.

Penalties for violating CFIUS regulations are significant and have recently increased. Effective December 26, 2024, CFIUS may impose civil penalties up to the greater of $5 million per violation or the transaction's value for failing to submit a mandatory filing, making material misstatements or omissions, submitting false certifications, or violating material terms of a mitigation agreement, order, or condition.

Key takeaways:

- **In the United States, the Committee on Foreign Investment in the United States (CFIUS) scrutinizes inbound investments in quantum companies for national security risk. This scrutiny can include intensive diligence, mitigation agreements, and potential divestiture requirements. The Foreign Investment Risk Review Modernization Act (FIRRMA) expanded CFIUS's jurisdiction and introduced mandatory filings in defined cases, and mitigation agreements, carveouts, and governance controls now regularly shape business transactions in the quantum sector.**
- **New "reverse CFIUS" measures are emerging to regulate outbound U.S. investments in sensitive quantum technologies abroad. These measures can require notifications, impose prohibitions on certain transactions, and increase enforcement risk for noncompliance.**
- **As these regulatory frameworks evolve, stakeholders in the quantum industry should understand the relevant laws and take proactive steps to ensure compliance. Early awareness and strategic planning can mitigate risks, facilitate smoother transactions, and support continued innovation in this rapidly advancing sector.**

5.1 COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

CFIUS protects U.S. national security by reviewing and, when necessary, blocking or mitigating foreign transactions and investments in U.S. companies that develop or possess critical technologies, including those in the quantum sector.

5.1.1 Foreign Investment Risk Review Modernization Act of 2018

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) broadened CFIUS's authority to scrutinize foreign investments in U.S. quantum technology companies, including minority stakes and real estate deals involving critical quantum research, infrastructure, or sensitive data. As a result, regulators subject quantum industry stakeholders to increased review and may restrict foreign capital, especially from countries of concern, to protect U.S. national security and technological leadership. FIRRMA modernized CFIUS procedures, introduced mandatory filings for certain transactions, and enhanced the government's ability to block or mitigate foreign investments that could threaten U.S. national security. (See also Key Aspects of the Interim Final Rule (IFR) Effective September 6, 2024 in Section 4.2 regarding IFR impacts on CFIUS)

5.1.2 Covered Control Transactions

Under CFIUS, a "covered control transaction" occurs when a foreign person obtains control of a U.S. business, including through a merger, acquisition, or takeover, and the deal could pose national security risks. CFIUS reviews these transactions and, where necessary, requires mitigation to address those risks.

5.1.3 Covered Investments

Under CFIUS, "covered investments" are certain non-controlling investments by foreign persons in U.S. businesses that deal in critical technologies, critical infrastructure, or sensitive personal data of U.S. citizens. An investment qualifies as covered if it affords the foreign investor access to material nonpublic technical information, board or observer rights, or involvement in substantive decision-making related to the business's sensitive activities.

5.1.4 Filing and Review Process

The CFIUS process begins when the parties to a covered transaction submit a voluntary notice or declaration. CFIUS then conducts an initial review, typically lasting 45 days, to assess national security risks. If concerns persist, CFIUS may open a further investigation of up to 45 additional days, which can lead to mitigation, approval, or referral to the President. CFIUS refers a transaction to the President if the parties and the government cannot address unresolved national security concerns through mitigation or existing laws. Only the President may block, suspend, or require divestment to protect U.S. national security interests.

5.1.5 Mitigation Measures

CFIUS imposes legally binding mitigation agreements or conditions on transaction parties to reduce national security risks posed by foreign investment. These measures may restrict foreign access to sensitive technology or data, modify governance or operations, and impose ongoing compliance, monitoring, and reporting obligations.

5.1.6 Excepted Investors

Under CFIUS, "excepted investors" are foreign persons or entities from designated "excepted foreign states" such as Australia, Canada, the United Kingdom, and New Zealand that meet specific ownership, control, and compliance tests. When those investors satisfy the tests, CFIUS excludes them from certain jurisdiction and mandatory filings for non-controlling covered investments and certain real estate transactions, reflecting those countries' robust national-security review regimes and cooperation with the United States. CFIUS still reviews any deal that could result in foreign control of a U.S. business, and investors lose excepted status if they fail to meet the criteria.

5.1.7 Violations

Penalties for violating CFIUS regulations are significant and have recently increased. Effective December 26, 2024, CFIUS may impose civil penalties up to the greater of $5 million per violation or the transaction's value for failing to submit a mandatory filing, making material misstatements or omissions, submitting false certifications, or violating material terms of a mitigation agreement, order, or condition. CFIUS also has expanded authority to obtain information from transaction parties and third parties, including through subpoenas. CFIUS determines penalty severity based on aggravating and mitigating factors, such as national security impact, intent, cooperation, and compliance history.

5.1.8 Impacts on Stakeholders

Stakeholders must navigate CFIUS with careful planning, strong compliance controls, and growing emphasis on partnerships with trusted domestic and allied entities. As quantum technologies mature and their strategic value rises, CFIUS's influence will remain significant and evolving.

For U.S. quantum startups and companies, heightened CFIUS scrutiny makes foreign funding, especially from China, harder to secure. Authorities may delay or block deals, which shrinks the investor pool and complicates exits. Compliance and diligence costs also rise.

- For foreign investors: Barriers and uncertainty deter capital. Authorities have required some investors to divest from U.S. quantum firms when transactions posed security risks.
- For academic institutions and research consortia: Restrictions on spinouts and joint ventures with foreign partners limit access to global capital, collaborators, and expertise.
- At the ecosystem level: Oversight slows capital formation and commercialization, shifting investment toward domestic and allied sources. Government programs help support critical technologies, but overall risk appetite remains cautious.

5.2 REVERSE CFIUS

5.2.1 Overview

"Reverse CFIUS" refers to the U.S. government's outbound investment security regime, which the Department of the Treasury implemented under Executive Order 14105, effective January 2, 2025. Unlike traditional CFIUS, which reviews inbound foreign investment, this program regulates certain outbound investments by U.S. persons into specified national security technologies and products in countries of concern, currently the People's Republic of China, including Hong Kong and Macau. Covered transactions either fall under a prohibition or trigger a post-closing filing within 30 days. The regime does not provide pre-clearance or case-by-case approval, and parties must comply through largely self-executing and self-reported processes.

The regime aims to keep U.S. capital and its accompanying intangible benefits, including managerial expertise, networks, credibility, and access to follow-on financing, from advancing sensitive capabilities in countries of concern. It targets three areas: semiconductors and microelectronics; quantum information technologies; and certain highly capable artificial intelligence systems.

Within these sectors, the rules identify specific covered activities and distinguish between prohibited and notifiable deals. Prohibitions include investments linked to advanced chip design, high-end fabrication and packaging, certain supercomputing, quantum computing and key components, and AI systems designed for exclusive military, intelligence, or mass-surveillance uses or trained above specified high-compute thresholds. Lower-tier activities, such as integrated circuit work below the most advanced thresholds or AI systems above a lower compute threshold or with certain sensitive end uses, are notifiable within 30 days of closing.

5.2.2 U.S. Persons

The rules apply to "U.S. persons," including U.S. citizens and permanent residents (wherever located), entities organized under U.S. law (including foreign branches), and any person in the United States. Obligations extend beyond direct investing: U.S. persons must take all reasonable steps to prevent controlled foreign entities from undertaking prohibited deals, and they may not "knowingly direct" a non-U.S. person to enter into a transaction that would be prohibited if undertaken by a U.S. person. Senior U.S. officers or directors at non-U.S. firms may need to recuse themselves from specific decisions to avoid liability.

5.2.3 Covered Transactions

"Covered transactions" include:

- Equity and contingent equity purchases
- Certain debt financings with profit participation, board rights, or other equity-like governance features
- Conversions of contingent equity acquired on or after the effective date
- Greenfield or brownfield investments that establish or cause engagement in covered activities
- Joint ventures anywhere with a person of a country of concern that will engage in covered activities
- Limited partner commitments to non-U.S. pooled funds likely to invest in covered foreign persons in the three sectors

5.2.4 Covered Foreign Person

The counterparty must be a "covered foreign person." This category includes entities in a country of concern that engage in covered activities, certain non-Chinese holding or affiliate structures that Chinese operations connect to through majority ownership, control, or concentrated revenue or expenses, and joint ventures with Chinese partners that will engage in covered activities. If the counterparty also engages in covered activities, U.S. rules categorically prohibit deals that involve parties on specified U.S. restricted lists (e.g., Specially Designated Nationals and Blocked Persons (SDN), Chinese Military-Industrial Complex Companies (CMIC), U.S. Department of Commerce's Bureau of Industry and Security (BIS) Entity List, Military End Users/Military-Intelligence End Users (MEU/MIEU).)

5.2.5 Exceptions

Key exceptions to outbound investment restrictions include:

- Investments in publicly traded securities and in registered funds (e.g., index funds, ETFs, mutual funds), provided the investor obtains no rights beyond standard minority protections
- Certain limited partner interests in pooled funds if de minimis or if the U.S. investor has binding assurances that its capital will not be used for prohibited or notifiable deals
- Derivatives that do not confer equity, asset, or governance rights
- Full buyouts that eliminate country-of-concern status
- Routine intracompany funding that maintains pre–January 2, 2025 activities without creating new covered activities
- Fulfillment of binding pre-effective-date capital commitments
- Certain passive outcomes in syndicated loan defaults

The Department of Treasury may grant case-by-case national-interest exemptions and may later recognize certain allied-country regimes for additional relief.

5.2.6 Violations

The government may impose civil fines for violation of the Executive Order in an amount up to the greater of $368,136 (inflation-adjusted annually) or twice the transaction's value. The government may pursue criminal penalties of up to $1 million and/or up to 20 years' imprisonment for willful violations. The government may also require unwinding or divestiture.

5.2.7 Impact on Stakeholders

Reverse CFIUS compels U.S. investors and companies to conduct rigorous diligence before investing in sensitive sectors in countries of concern, thereby increasing costs, causing delays, or blocking deals.

Examples:

- A U.S. venture fund backing a Chinese AI startup may face a notification requirement or a prohibition if the technology is deemed sensitive
- Multinationals may restructure supply chains or investment plans to avoid covered activities, e.g., a chipmaker reconsidering expansion in China
- Tech firms may benefit from reduced risk of sensitive know-how transfer but face constraints on foreign market access or partnerships, such as limits on joint ventures with Chinese counterparts

Overall, while the regime aims to protect U.S. national security, it introduces new compliance burdens and strategic uncertainties for investors, corporations, and technology firms involved in cross-border activities.

Key Considerations: Foreign Investment Controls

CFIUS Compliance

Quantum industry participants engaged in cross-border transactions may choose to adopt a proactive and structured approach to CFIUS compliance. By systematically assessing jurisdiction, conducting due diligence, determining filing requirements, preparing comprehensive filings, cooperating with CFIUS, maintaining ongoing compliance, and engaging experienced counsel, parties can take steps to manage regulatory risk and support the continued growth and innovation of the quantum sector.

- **Assess CFIUS jurisdiction and risk.** Parties may first determine whether the transaction falls within CFIUS jurisdiction. This assessment analyzes whether the transaction involves a "U.S. business" and a "foreign person" as defined by CFIUS regulations. One important factor is whether the U.S. business engages in critical technology, critical infrastructure, or the handling of sensitive personal data, collectively referred to as a TID U.S. business. TID stands for "Technology, Infrastructure, and Data," and means a U.S. business involved in one or more of the following: critical technologies, critical infrastructure, or sensitive personal data. Each element has specific implications for quantum companies.

  Under CFIUS regulations, critical technologies include items subject to U.S. export control laws, including items on the Commerce Control List under the EAR, the U.S. Munitions List under the ITAR, and emerging and foundational technologies identified by the Department of Commerce.

  Critical infrastructure consists of systems and assets so vital to the United States that their incapacity or destruction would debilitate national security, economic security, or public health and safety. Quantum technologies already integrate into critical infrastructure sectors such as telecommunications, energy, and financial services, particularly as quantum communication networks and quantum-enhanced sensors proliferate. A quantum company that provides products or services essential to the functioning of critical infrastructure may qualify as a TID U.S. business on this basis.

The third prong of the TID definition covers the collection or maintenance of sensitive personal data of U.S. citizens. While this basis will less-commonly apply to quantum companies, it can apply if a QIST business collects or processes large volumes of sensitive personal data in connection with its products or services, including quantum-enhanced cybersecurity solutions or data analytics platforms.

Parties may also choose to evaluate the nationality and ownership structure of the foreign investor, including any government ownership or influence, because these factors can significantly increase CFIUS scrutiny.

- **Conduct comprehensive due diligence.** Parties can conduct thorough due diligence to understand the rights and access the foreign investor will obtain through the transaction. This review may include an evaluation of access to nonpublic technical information, board or observer rights, and participation in substantive decision-making. Parties can also identify any export-controlled technologies or government contracts associated with the U.S. business, as these elements can elevate CFIUS risk and trigger additional regulatory requirements.

- **Determine filing requirements.** Parties can assess whether the transaction triggers a mandatory CFIUS filing. A filing is mandatory when a foreign government acquires a substantial interest in a TID U.S. business or when the transaction involves critical technologies subject to export controls. Even when a filing is not mandatory, parties may desire to consider a voluntary filing to obtain a safe harbor from future CFIUS intervention and reduce regulatory uncertainty.

- **Prepare and submit the CFIUS filing.** Parties may gather detailed information about the transaction, the U.S. business, the foreign investor, and all relevant ownership structures to prepare the filing. Depending on the complexity and risk profile, parties may submit a short-form declaration or a full notice. All filings are to be submitted through the Treasury Department's online portal and ensure accuracy and completeness to avoid delays or additional scrutiny.

- **Respond to CFIUS review.** After submitting a filing, parties could benefit from cooperating with CFIUS and responding promptly to requests for additional information or clarification. If CFIUS identifies national security concerns, parties may need to negotiate and implement mitigation measures, including limiting foreign access to sensitive information, appointing U.S. citizen board members, and establishing robust security protocols.

- **Maintain ongoing compliance.** For transactions subject to mitigation agreements, ongoing compliance and reporting is to be maintained, including keeping thorough records of the transaction CFIUS filings. Doing so can demonstrate adherence to regulatory obligations and to facilitate future reviews or audits.

- **Engage experienced legal counsel.** Given the complexity and evolving nature of CFIUS regulations, engaging experienced legal counsel can be beneficial. Counsel can provide guidance in assessing CFIUS risks, preparing filings, and navigating the review process to ensure compliance and support timely transaction execution.

Reverse CFIUS

Reverse CFIUS compliance requires quantum companies to proactively assess and monitor outbound investments and collaborations involving foreign counterparties. Effective compliance requires rigorous diligence, prompt reporting, and ongoing engagement with regulatory authorities to ensure that outbound investments do not compromise national security or violate U.S. regulations. Impacted entities should:

- **Determining applicability.** A structured compliance program that manages outbound investment restrictions and related disclosure obligations starts by determining applicability. First, confirming whether the investor qualifies as a U.S. person—a citizen, lawful permanent resident, U.S. entity, or individual physically present in the United States—may be warranted. Next, an assessment of whether the counterparty qualifies as a covered foreign person—such as a Chinese entity, individual, or government actor, or an entity majority-owned or controlled by such persons—may also be required. In addition, confirming that the contemplated transaction involves a covered sector, including semiconductors, quantum technologies, or artificial intelligence may also be beneficial.

- **Conducting comprehensive due diligence.** An evaluation of whether the target engages in covered activities within the quantum domain, such as advanced quantum computing, enabling hardware, cryogenic control systems, quantum sensors tied to national-security use cases, or associated software and services can be part of conducting due diligence. Mapping direct and indirect ownership, including fund structures and co-investors can be beneficial. Parties may also wish to consider conducting a reasonable and diligent inquiry using public and commercial databases, obtain contractual representations and warranties, and review all reasonably available information that bears on covered activities and beneficial ownership.

- **Classifying the transaction.** If an activity is prohibited, applicable law calls for U.S. persons to prevent controlled foreign entities from entering the transaction. If the transaction is notifiable, a file can be submitted to the U.S. Department of the Treasury within 30 days of closing. If an exception applies, a filing would not be required; however, consider retaining documentation supporting the exemption.

- **Notifying the Department of the Treasury.** For notifications, a submission can be filed with the Department of Treasury's Office of Global Transactions. The filing typically includes details about the U.S. person, the transaction structure and timing, the covered foreign person, the commercial rationale, and the specific covered activities implicated, with sufficient technical description for quantum-related capabilities and end uses.

- **Maintain ongoing compliance.** Compliance is also warranted after closing. If later discovered that a transaction was notifiable or prohibited, notification to Treasury within 30 days of discovery is called for by applicable law. Post-closing monitoring of investments for changes in business activities, capabilities, ownership, or control can aid in evaluating notification requirements and prohibitions. Corrections of material omissions or inaccuracies in a prior notification may also be required.

- **"Knowingly directing" prohibited transactions.** Knowingly directing prohibited transactions violates applicable law. U.S. persons may not instruct or facilitate non-U.S. persons to undertake transactions that would be prohibited if conducted by a U.S. person. Where relevant, the following items can be considered when evaluating compliance strategy: recusing from decision-making, implementing information barriers, and deploying governance controls to mitigate liability, particularly in global funds and multinational corporate structures active in quantum technologies.

6 | America First Trade Policy and Tariffs

WHY THIS MATTERS FOR THE QUANTUM SECTOR

The America First Trade Policy has fundamentally reshaped the landscape for the QIST and other advanced technology stakeholders as policymakers have made tariffs a central tool to promote domestic manufacturing, protect intellectual property, and address perceived trade imbalances. While these measures aim to strengthen national security and economic competitiveness, they also introduce new complexities and risks for the QIST sector, which depends on a fragile, internationally integrated network of suppliers and collaborators. Tariffs on critical imports, ranging from photonic components to cryogenic hardware, raise costs, disrupt sourcing, extend research timelines, and delay projects in every stage of quantum innovation and at organizations from small startups to large enterprises.

The quantum technology supply chain faces unique vulnerability to global trade disruptions, particularly tariffs. Unlike more mature industries, quantum system developers rely on a narrow set of highly specialized components and materials. These components include ultra-pure metals, rare earth elements, precision optics and lasers, cryogenic systems, high-frequency electronics, specialty isotopes, and advanced vacuum and machining technologies. Because a small, globally distributed supplier base supports the industry, even minor cost or timing shocks propagate rapidly and affect research, development, and commercialization across the sector.

Key takeaways:

- **The resulting volatility hits organizations with limited resources especially hard, and even the largest players face increased operational complexity and compliance burdens.**
- **The quantum sector may respond with a diverse array of mitigation strategies, including tariff engineering, dual sourcing, modular system design, collaborative procurement, and long-term supplier partnerships. These approaches, grounded in legal expertise and supply chain innovation, help buffer the most severe impacts and lay the groundwork for a more resilient industry.**
- **The path forward for the quantum supply chain may warrant continued adaptation and proactive investment. Stakeholders may seek to deepen regional and allied partnerships, invest in domestic manufacturing capacity, and foster greater transparency and agility throughout the supply chain.**
- **Policymakers, in turn, may find it beneficial to consider balancing the goals of economic security with the need to maintain global collaboration and access to critical technologies. By embracing these principles, it may be possible for the U.S. quantum industry to weather the current era of trade uncertainty and also build a robust, innovative, and secure foundation for the quantum technologies that will define the future.**

6.1 AMERICA FIRST TRADE POLICY AND TARIFFS

The America First Trade Policy marks a significant shift in U.S. trade strategy, emphasizing domestic industrial strength, technological leadership, and national security. At its core, the policy seeks to reduce the U.S. trade deficit, counter perceived unfair foreign trade practices, and reshore critical manufacturing capabilities. Tariffs, both broad-based and sector-specific, serve as the central tool used to try to achieve these goals, and the administration has imposed sweeping new duties on imports from China, Mexico, Canada, and other trading partners, as well as targeted tariffs on strategic sectors such as semiconductors, electronics, and advanced technology components. The policy also seeks to strengthen customs enforcement, tighten rules of origin, and advance a push for domestic manufacturing incentives.

Under the new tariff regime, U.S. import duties have increased on many specialized components essential to quantum systems, including ultra-pure metals, precision optics, cryogenic equipment, and high-frequency electronics. Section 301 tariffs on Chinese electronics and optical instruments, Section 232 tariffs on steel and aluminum, and retaliatory tariffs from other countries have added to increased costs and heightened volatility for quantum hardware manufacturers and research institutions. In response, the industry has had to qualify alternative suppliers, manage longer lead times, and absorb price shocks. These challenges are exacerbated by the global and highly specialized nature of quantum technology supply chains.

Policymakers aim to ensure that the United States maintains its edge in quantum science and commercialization, even as the global landscape becomes more fragmented and competitive. They recognize quantum technologies as foundational to future U.S. economic competitiveness and national security, and the government explicitly identifies quantum as a strategic priority. The America First Trade Policy accompanies calls for expanded federal investment in quantum research and development, quantum workforce development, and regional tech hubs, as well as continued efforts to coordinate with allies on technology standards.

But the immediate effect of the America First Policy has been increased costs, disrupted supply chains, and additional compliance complexities for quantum companies, startups, and research labs.

6.2 IMPACTS ON STAKEHOLDERS

Examples of impacts by the America First Trade Policy on stakeholders include:

- **Cost Increases and price volatility.** Tariffs disproportionately affect the quantum supply chain due to its thin supplier base and the high value of individual components. When tariffs of 10 to 25 percent apply to critical items such as lasers, single-photon detectors, precision motion stages, or radio frequency and microwave modules, the total system cost often rises by double-digit percentages. The lack of substitute suppliers and the slow, expensive process of qualifying alternatives limit the ability of quantum companies and labs to hedge against these increases.

- **Disruptions to sourcing and procurement.** Tariffs introduce complexity into sourcing and procurement and require companies to navigate tariff classification and rules-of-origin issues. Even small design changes shift tariff exposure and force firms to re-source or redesign products. U.S. Customs and Border Protection reviews and tariff complexity add paperwork and lengthen port dwell times, which leads to longer lead times for mission-critical parts. Supplier concentration risk intensifies when a country becomes subject to tariffs, as companies rush to qualify second sources that may not meet performance specifications.

- **Effects on research, development, and commercialization timelines.** The specialized nature of quantum hardware means delays in the arrival of a single component, such as a cryogenic amplifier, a high-numerical-aperture objective, or an ultra-stable laser, which may stall experiments and system integration for weeks. Swapping out tariffed parts often requires new calibration, thermal modeling, electromagnetic interference testing, and reliability validation, which stretches project milestones. Budget shocks are common; grant-funded labs and fixed-price contracts must re-scope experiments or reduce deliverables when parts overrun budgets. Tariff-driven changes to the bill of materials also delay certification and factory acceptance testing, which postpones product launches.

- **Impact on small businesses, startups, and large enterprises.** The impact of tariffs falls differently across the quantum ecosystem. Small businesses and academic labs struggle most to absorb cost spikes due to limited purchasing power and inventory. Grant cycles and price caps constrain their flexibility, so higher duties often directly reduce the number of experiments or system capability.

  Large enterprises are better equipped to mitigate tariff impacts through multi-sourcing, in-house machining, and bonded warehouses, but they face complex global compliance and transfer-pricing challenges. Some shift final assembly to tariff-favorable jurisdictions, increasing overhead and operational complexity. For instance, a multinational corporation rebalanced manufacturing of control racks to Mexico and the EU to reduce tariff exposure, which incurred new product introduction transfer costs but stabilized margins.

In summary, tariffs amplify both the financial and operational risks facing the quantum industry and threaten to slow innovation and disproportionately strain the most agile and resource-constrained players. Addressing these challenges requires coordinated mitigation strategies and policy solutions to ensure the continued advancement of quantum technologies.

Key Considerations: Tariff Mitigation Strategies

As tariffs disrupt the flow and cost structure of critical inputs, quantum companies, research labs, and startups have adopted sophisticated mitigation strategies. Operational necessity drives these strategies, and a complex landscape of international trade laws, export controls, and customs regulations that govern the movement of quantum-enabling technologies also shapes them.

- **Tariff engineering and HS code optimization.** One of the most impactful mitigation tactics is tariff engineering, which involves structuring products or shipments to qualify for lower tariff rates under the Harmonized System (HS) of classification. Quantum companies often work closely with legal counsel and customs experts to analyze the technical specifications, composition, and intended use of each component.
- **Dual sourcing and regionalization.** To reduce exposure to country-specific tariffs and supply chain shocks, quantum organizations increasingly pursue dual sourcing and regionalization strategies. This approach means qualifying multiple suppliers for critical components, such as high-stability lasers, vacuum chambers, or RF modules, across different jurisdictions.
- **Design-for-substitution and modular architectures.** Given the risk of sudden tariff changes or export restrictions, quantum system designers increasingly adopt design-for-substitution principles. They create modular system architectures with standardized interfaces so that key components, such as cryogenic amplifiers, timing modules, or photonic chips, can be swapped with minimal requalification if a supplier becomes subject to tariffs or export controls.
- **Long-term contracts and vendor-managed inventory.** To buffer against price volatility and supply chain disruptions, many quantum companies negotiate longer-term contracts with key suppliers and implement vendor-managed inventory (VMI) programs. By locking in prices and delivery schedules for critical items, such as dilution refrigerators or superconducting wire, organizations can reduce exposure to sudden tariff hikes or shortages. These contracts often use international commercial terms (Incoterms) and require careful attention to customs valuation rules and anti-dumping regulations.
- **Collaborative procurement and consortia.** Collaborative procurement through industry consortia or national laboratories can provide quantum organizations with scale advantages and increased bargaining power. By aggregating demand, research institutions and industry groups can negotiate better terms with suppliers and, in some cases, secure tariff exemptions for research or educational purposes.

Effectively mitigating tariff risks in the quantum supply chain may warrant a multifaceted, proactive approach that blends legal expertise, supply chain agility, and collaborative action. Navigating the interplay of trade laws, export controls, and customs regulations can be essential for maintaining resilience and supporting the continued advancement of quantum technologies. As tariffs amplify cost and schedule risks, especially given the specialized nature of quantum components and the slow pace of supplier qualification, these strategies can be vital in ensuring that startups, research labs, and large enterprises can continue to innovate and compete in a rapidly evolving global landscape.

7 | Global Talent and Immigration

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Attracting and retaining world-class talent is essential for U.S. quantum labs, startups, and manufacturers to innovate and compete. Building a robust, quantum-ready domestic talent pool through education and workforce development programs at all levels is key—and public funding at both national and subnational levels is crucial to advancing this mission. Still, international expertise remains an important source of talent, making it important that quantum employers understand the applicable laws and regulations.

Foreign nationals make up about one quarter of the U.S. STEM workforce and the majority of graduate students in quantum-adjacent fields such as physics, electrical engineering, and computer science. Quantum teams in the United States routinely employ international PhD candidates, postdocs, and specialists using the following visa categories: F-1 STEM OPT, J-1 research programs, H-1B specialty occupations, O-1 extraordinary ability, and employment-based green cards such as EB-1 and EB-2 National Interest Waiver (NIW).

A tightening immigration policy environment constrains access to this talent. Visa caps, higher fees, stricter adjudications, extended security vetting, and backlogs delay hiring and scale-up. Export controls, including deemed-export rules under EAR, ITAR, and related sanctions; research security requirements such as National Security Presidential Memorandum 33; investment reviews under CFIUS; and the CHIPS guardrails relating to immigration impact can determine who may access equipment, data, and funding, and who may not.

Quantum employers can utilize proactive immigration planning and rigorous compliance so they can recruit, retain, and lawfully deploy international experts and specialists without disrupting research or commercialization.

Key takeaways:

- **Quantum employers who hire international talent can benefit from a clear view of core visa pathways, which includes evaluating caps, backlogs, and compliance risks.**
- **Immigration choices directly affect export controls, research security obligations, and investment reviews. Recruiting and deployment strategies can be established to protect research, funding, and commercialization.**
- **When employers implement an integrated approach effectively, they may be able to turn compliance into a competitive advantage. This approach can accelerate hiring, safeguard IP and sensitive data, and reinforce U.S. leadership in quantum.**

7.1 KEY U.S. IMMIGRATION LAWS

7.1.1 The Immigration and Nationality Act and Code of Federal Regulations

The Immigration and Nationality Act (INA), codified mainly at Title 8 of the United States Code, and its implementing regulations in the Code of Federal Regulations (primarily at 8 C.F.R.), constitute the core legal framework for U.S. immigration. These laws define the visa categories, admission and removal procedures, permanent residency (green card) rules, and naturalization processes that enable quantum companies to recruit and retain international talent essential for research, development, and innovation.

7.1.2 Federal Departments and Agencies

The Department of Homeland Security (DHS) administers and enforces most immigration laws, sets policy, and coordinates its component agencies in enforcement. For the quantum industry, DHS shapes the policies that affect the hiring and mobility of international scientists, engineers, and other specialized professionals.

Within DHS, U.S. Citizenship and Immigration Services (USCIS) adjudicates immigration benefits inside the United States, including petitions and applications for visas (such as H-1B and O-1 for highly skilled workers), adjustment of status, employment authorization, humanitarian programs, and naturalization, and these functions are critical for quantum companies that seek to employ foreign talent.

U.S. Customs and Border Protection (CBP) inspects and admits travelers at ports of entry, enforces immigration and customs laws at and between ports, and determines whether arriving noncitizens may enter the United States, including quantum professionals who come for work or conferences.

Immigration and Customs Enforcement (ICE) enforce immigration laws in the interior through investigations, detention, and removal operations, and it runs compliance programs such as worksite enforcement that help quantum industry employers meet employment eligibility and verification requirements.

7.2 U.S. IMMIGRATION OPTIONS (NONIMMIGRANT AND IMMIGRANT)

The expanding quantum industry in the United States attracts top global talent, making an understanding of U.S. immigration options essential for professionals and organizations in this field. The United States provides both nonimmigrant (temporary) and immigrant (permanent) visa pathways to accommodate a range of needs.

Nonimmigrant visas, such as the H-1B for specialty occupations, O-1 for individuals with extraordinary ability, L-1 for intracompany transferees, and F-1 or J-1 for students and researchers, allow quantum professionals to work, study, or collaborate in the United States on a temporary basis.

The primary avenues for those seeking permanent residence are employment-based green card categories like EB-1 (extraordinary ability or outstanding researchers), EB-2 (advanced degree or exceptional ability, including National Interest Waiver), and EB-3 (skilled professionals). Family-based and investment-based options may also apply in certain situations.

Key considerations for both nonimmigrant and immigrant options include eligibility criteria, intent, numerical limits and backlogs, the need for employer or family sponsorship, and timing.

7.2.1 Nonimmigrant Options

- **H-1B (Specialty Occupation).** The H-1B remains the canonical choice for early-career quantum scientists who hold at least a bachelor's degree (or its equivalent) in a specialty field such as quantum physics, electrical engineering, or computer science. The statute sets a strict annual numerical cap of 65,000 visas and adds 20,000 additional slots for holders of U.S. advanced degrees. USCIS conducts selection through a randomized electronic lottery that typically runs in March. After selection, USCIS can adjudicate the petition in as few as 15 calendar days with premium processing. The employer's filing of the Labor Condition Application, through which the employer attests that it will pay the "required wage" (the higher of the prevailing or actual wage for the occupation in the area of intended employment), typically adds roughly ten business days to the timeline.

  Universities, nonprofit research organizations, and their qualified affiliates enjoy cap-exempt status, which allows them to file year-round. Quantum laboratories and consortia frequently use this option.

The government may approve an initial period of up to three years and renew the H-1B to a maximum of six years. During this time, the beneficiary may pursue an employer-sponsored or self-petitioned permanent residency application, and the doctrine of "H-1B portability" allows the beneficiary to continue working when changing employers once the new employer files a petition.

ALERT: One potential challenge with the H-1B program arises from changes to the lottery selection process. As of October 2025, the White House has proposed significant changes to the way H-1B applications are selected in the annual lottery. Specifically, the DHS, which oversees this process, has proposed a selection method that places greater emphasis on the wages offered to a foreign national. The proposal would make it more difficult to select entry-level quantum researchers since most entry-level positions, by definition, fall on the lower end of the pay scale. The proposal may also chill the population of international students in the U.S. due to the increasing difficulty, whether real or perceived, of obtaining a post-graduation work visa in the U.S. This regulatory change remains a proposal. If finalized, implementation would likely apply to the fiscal year 2027 H-1B cap season beginning in March 2026.

Another challenge that the H-1B program faces under the current U.S. administration involves ongoing attempts to alter the program outside the normal regulatory process. For example, the White House issued a Presidential Proclamation on September 22, 2025, purporting to impose a new $100,000 fee on "new" H-1B petitions filed on or after September 24, 2025. Given the diverse ways employers file H-1B applications, they remain deeply uncertain about whether routine applications for portability, or cap-exempt requests for new H-1Bs, for example, fall within this Proclamation. While the legality of the Proclamation is being litigated, employers do face new and unknown hurdles when they attempt to use this program to hire highly skilled workers.

- **O-1A (Extraordinary Ability).** When a quantum professional has established a record of sustained acclaim (i.e. peer-reviewed publications with high citation counts, invited talks at top conferences, fundamental patents, or prestigious awards) the O-1A offers a cap-exempt, prevailing-wage-free alternative.

  This classification requires evidence that the beneficiary belongs to the small percentage at the very top of the field, as shown through at least three regulatory criteria or a major internationally recognized prize. Adjudications typically take two to four months, but premium processing guarantees a 15-day decision, which makes the O-1A invaluable for time-sensitive projects such as DARPA-funded quantum prototypes. The visa can be approved for up to three years and can be extended in one-year increments without a statutory limit. When the petitioner characterizes the request as a new event, an extension can be valid for three more years.

  Although the O-1A does not itself confer immigrant intent, the EB-1A immigrant classification (extraordinary ability) (discussed in section 7.2.2) naturally complements it, and evidentiary standards for both applications substantially mirror each other, which creates a comparatively seamless bridge to a green card without the Program Electronic Review Management (PERM) labor-market test—a process whereby employers demonstrate they've made an effort to find qualified domestic workers for a job before hiring a foreign national. That said, an O-1A approval does not guarantee approval of the corresponding green card category, and researchers may need to build their credentials patiently to secure permanent residence in the U.S.

- **L-1 (Intra-Company Transferee).** Global quantum companies now deploy the L-1 to rotate key talent from foreign research hubs into U.S. operations. The beneficiary must have worked for a related foreign entity for at least one continuous year within the three preceding years in an executive or managerial (L-1A) or specialized knowledge (L-1B) capacity. No annual quota or prevailing wage requirement applies, which makes budgeting more predictable for startups that have not secured venture funding. Regular processing takes two to five months, but blanket L adjudications at consulates and premium processing of individual petitions compress timelines to days.

  L-1A executives and managers can convert to EB-1C permanent residence without a labor certification after one year in the United States, whereas employers typically sponsor L-1B specialized-knowledge employees for EB-2 or EB-3 permanent residence pathways.

  One practical challenge faced by Indian and Chinese professionals applying for L-1Bs, often referred to as the individual contributor L-1 visa, results from the difficulty of securing permanent residence within the five-year cap on these visas due to country quotas. As a result, companies often seek to switch these employees to an H-1B visa because country quotas allow extensions of H-1B status beyond the six-year limit. The earlier referenced H-1B lottery creates uncertainty for individuals from these backlogged countries.

- **E-2 (Treaty Investor/Employee).** Nationals of countries that maintain qualifying bilateral investment treaties with the United States may obtain an E-2 by investing, or by being employed by a company that has invested, a substantial yet flexible amount of capital in a bona fide U.S. enterprise. This classification particularly attracts quantum startups founded by European, Japanese, or Australian scientists whose home governments subsidize quantum research and development and thus satisfy nationality requirements.

  Consular officers usually conclude adjudication within a few months after document submission, and no numerical ceiling or prevailing wage mandates apply. Consulates issue visas for up to five years depending on reciprocity schedules.

  While the E-2 may be renewed indefinitely, it lacks a direct statutory pathway to permanent residence. Additionally, this category technically requires a founder to demonstrate the intent to eventually return home. Many founders who seek permanent residence transition into EB-5, EB-1C, or NIW categories once the enterprise matures, but they must evaluate how that transition affects their underlying E-2 status.

- **J-1 (Research Scholar).** Universities and national laboratories frequently rely on the J-1 to host post-doctoral quantum researchers for up to five years. The sponsoring institution issues Form DS-2019, and consular officers typically process the visa swiftly, subject only to security-clearance delays for sensitive technologies. Although no wage floor governs the program, sponsors must show adequate financial support.

  Some scholars become subject to the two-year home-residency requirement under INA section 212(e), particularly when their governments fund them or when they work in fields listed on the Exchange Visitor Skills List. A waiver, obtainable through a no-objection statement, an interested-government-agency endorsement (for example, from the National Science Foundation or the Department of Education), or an exceptional hardship claim, generally serves as a prerequisite to shifting into H-1B or immigrant status. The J-1 does not provide a long-term visa and requires an intent to return home. Sponsors should reserve it for short-term situations.

- **F-1 STEM OPT Extension** International students who graduate from U.S. institutions with degrees in qualifying STEM fields, including quantum physics, applied mathematics, and quantum information science, may remain for an initial 12-month period of Optional Practical Training and may extend by an additional 24 months under the STEM OPT rule. The employer must enroll in E-Verify and execute Form I-983, articulating a training plan and a wage commensurate with similarly situated U.S. workers, though no formal prevailing wage calculation is required. U.S. Citizenship and Immigration Services typically adjudicates requests in 60 to 90 days, and the cap-gap provision bridges employment authorization through September 30 each year when the employer has timely filed an H-1B change-of-status petition.

ALERT: The DHS has proposed a new regulation that would change how long international students may stay in the U.S. While the rule is not yet final, it could require international students to apply more frequently for extensions of status in the U.S. and could cause additional disruptions.

- **E-3 (Australian Citizens):** The E-3 visa is a U.S. nonimmigrant category for Australian citizens to work in a specialty occupation requiring highly specialized knowledge and at least a bachelor's degree (or equivalent) in a specific field. It is employer-sponsored, requires a certified Labor Condition Application (LCA) confirming the prevailing wage and working conditions, and is typically granted in renewable two-year increments. The E-3 is similar in design to the H-1B, with overlapping requirements. However, several important distinctions include the following: there is an annual cap of 10,500, which historically is not reached and therefore is rarely an obstacle; Australians can apply directly for E-3 visas at a U.S. consulate overseas, avoiding USCIS petition filing fees; E-3 visas are issued in two-year increments and can be renewed indefinitely; and the E-3 is not a dual-intent visa, which can complicate sponsorship for permanent residence.

- **H-1B1 (Chilean and Singaporean Citizens):** The H-1B1 is a U.S. nonimmigrant category for citizens of Chile and Singapore to work in a specialty occupation requiring highly specialized knowledge and at least a bachelor's degree (or equivalent). It is employer-sponsored and requires a certified Labor Condition Application (LCA) confirming the prevailing wage and working conditions. Like the E-3, it overlaps with the H-1B in its legal requirements but is distinguishable in several important ways. It is subject to a 6,800-visa set-aside for Chile and Singapore that has historically been underutilized. H-1B1 status is issued in one-year increments with indefinite renewals. It requires clear nonimmigrant intent, which is stricter than the H-1B's tolerance for dual intent. Individuals can apply directly for H-1B1 visas at a U.S. consulate, eliminating the need to pay USCIS filing fees. Additionally, dependents are not eligible for work authorization.

- **TN (Canadian and Mexican Citizens):** The TN is a U.S. nonimmigrant classification under the USMCA for citizens of Canada or Mexico to perform prearranged, professional-level work in one of the treaty's listed professions (for example, Engineer, Physicist, Mathematician, Computer Systems Analyst, University Teacher, Research Assistant), with the required degree/credentials as specified for that profession. Key features of this classification include: it is employer-specific and prohibits self-employment; there is no LCA/prevailing wage requirement and no quota; it requires temporary (nonimmigrant) intent and is granted for up to three years at a time, with unlimited three-year extensions; and dependents (TD) may accompany the principal but are not authorized to work. Canadians typically apply for TN status at a port of entry without a visa, while Mexicans must obtain a TN visa at a U.S. consulate before admission.

7.2.2 Immigrant Options:

- **EB-1 and EB-2 National Interest Waiver (Permanent Residence).** For quantum professionals seeking a direct route to a green card, the first-preference EB-1A (extraordinary ability) and EB-1B (outstanding researcher/professor), as well as the second-preference EB-2 NIW, are the principal tools.

  Petitioners file EB-1 cases to bypass the labor certification and, in most instances, rely on current visa-bulletin priority dates, which allows USCIS to approve the petition in roughly eight to twelve months with premium processing and, for applicants not chargeable to India or China, to adjudicate adjustment of status within that timeframe.

The EB-2 NIW, modified by the "Matter of Dhanasar" precedent, requires the applicant to show that the proposed endeavor has substantial merit and national importance, that the applicant is well-positioned to advance the endeavor, and that waiving the labor-market test would benefit the United States. Quantum technologies typically meet these prongs, although an individual must satisfy these criteria based on the applicant's individualized accomplishments. Although EB-2 visas are numerically capped and per-country quotas create backlogs for certain nationalities, premium processing reduces petition adjudication to 45 days, which brings more predictability to long-term hiring plans.

7.3 U.S. IMMIGRATION SYSTEM CHALLENGES

The U.S. immigration system is known for its complexity and frequent rule changes. This dynamic environment forces individuals and organizations to work hard to stay current and compliant. Applicants must navigate numerous visa types, each with its own requirements, documentation, and timelines. Even minor errors in the application process can cause significant delays or outright denials, which adds to applicants' frustration and uncertainty.

Lengthy and unpredictable processing times rank among the most daunting aspects of the U.S. immigration process. Agencies may take many months or even years to approve a visa or work authorization. This unpredictability disrupts hiring plans, research initiatives, and business operations, which makes it extremely challenging for organizations and individuals to plan with confidence.

Strict eligibility requirements further complicate the process. Many visa categories require applicants to meet specific criteria, such as holding certain educational qualifications, having a job offer, or meeting minimum salary thresholds. As a result, even highly qualified candidates may become ineligible if they fall short of a single requirement, which limits access to global talent and hinders organizations' ability to recruit the best candidates.

Quotas and caps present another significant barrier. Certain visa categories, such as the H-1B for skilled workers, face annual numerical limits. When applicants exceed the available slots, agencies distribute visas by lottery. This system leaves many qualified individuals without a pathway to work in the United States, regardless of their skills or employers' needs.

The intensifying political climate surrounding immigration in the United States creates real reputational risk for employers. Immigration policy is a focal point of national debate, and companies must remain especially vigilant when using visa sponsorships to address talent shortages. Any violations of visa requirements can trigger negative publicity and reputational damage that may be difficult to overcome.

The risk of non-compliance with immigration rules remains ever-present. The law requires both employers and individuals to adhere to complex regulations and maintain meticulous records. Mistakes or misunderstandings can lead to severe consequences, including financial penalties, loss of visa status, or even bans on future applications. These high stakes underscore the importance of careful management and expert guidance when navigating the U.S. immigration system.

Beyond procedural and legal challenges, immigration processes can deeply stress individuals and their families. Applicants may endure long periods of separation from loved ones, uncertainty about their future in the United States, or difficulties with work and school while waiting for approvals. This personal and family uncertainty can take a significant emotional toll and impair well-being and productivity.

Finally, these immigration challenges broadly impact innovation and collaboration. Lengthy delays, strict requirements, and unpredictable outcomes can slow critical projects, make it harder for organizations to attract and retain top global talent, and limit opportunities for international collaboration. These factors carry particular consequences in fast-moving and highly competitive fields like quantum technology, where success depends on quickly assembling diverse, world-class teams and working across borders.

Key Considerations: Immigration

The quantum industry's continued growth and global competitiveness depend heavily on access to top-tier international talent. A robust immigration strategy attracts, retains, and integrates scientists, engineers, and specialists who drive advancements in quantum computing, sensing, and communications. Parties may implement certain practices to address immediate workforce needs and strengthen the long-term foundation of the industry.

- **Specialized categories.** Leveraging specialized visa categories strategically can be an effective strategy. Matching roles to appropriate visas such as H-1B for specialty occupations, O-1A for individuals with extraordinary ability, L-1A or L-1B for managers and those with specialized knowledge, TN for Canadian and Mexican professionals, E-3 for Australians, J-1 for research scholars and interns, and H-1B1 for citizens of Chile and Singapore, can help employers bring the right talent on board efficiently. Cap strategies including targeting cap-exempt H-1Bs through qualifying nonprofits or universities and using concurrent H-1B employment to bridge cap-exempt and cap-subject roles, also helps employers navigate annual limitations. Fast-tracking options, including premium processing, selecting consular posts with better appointment availability, and utilizing blanket L petitions for multinationals, can further streamline the process. For example, a quantum algorithm lead with high-impact citations and invited talks may be able to pursue an O-1A visa, while embedded systems engineers from a Canadian partner could possibly enter under the TN category as the company pursues H-1B slots through the lottery.

- **Global talent pipelines.** Companies may find it beneficial to build early, global talent pipelines. Sourcing talent at international conferences such as Q2B and APS March Meeting, as well as from quantum PhD programs and national laboratories, can result in identifying future leaders in the field. Co-sponsoring competitions and hackathons and creating targeted fellowships, internships, and visiting researcher tracks—aligned to export-control-safe project areas—may further expand the pool of qualified candidates. For instance, a firm may be able to fund a joint PhD fellowship with a European university and set up F-1 pathways for summer and postdoctoral roles.

- **F-1 OPT and STEM OPT programs.** Maximizing the use of F-1 OPT and STEM OPT programs can enable employers to hire international graduates from U.S. universities. Careful planning of timelines, combining 12 months of OPT with a 24-month STEM extension, and aligning E-Verify and training plans, such as Form I-983, are key steps. Staging roles to begin with non-controlled projects simplifies onboarding, with a transition to long-term statuses before the final year of STEM OPT. As an example, a quantum software graduate can start on OPT in benchmarking, and by month twelve, the employer may file an EB-2 NIW petition to support continuity of employment.

- **Green card strategies.** Designing green card strategies around talent tier and timelines can aid in permitting critical personnel to remain in the U.S. long term. The EB-1A for extraordinary ability and EB-1B for outstanding researchers fit top scientists, while the EB-2 NIW fits mission-critical work, and PERM under EB-2 or EB-3 covers broader roles. Sequencing filings to reduce risk, such as parallel O-1A and EB-1A or NIW applications and early I-140 filings to enable H-1B extensions beyond six years and H-4 EAD eligibility for dependent spouses may provide stability. For example, a quantum error-correction researcher with seminal citations may be able to target EB-1A, while a cryo-hardware engineer could possibly pursue EB-2 PERM.

- **Compliance and audit readiness.** Maintaining rigorous compliance and audit readiness may avoid delays and penalties. Implementing controls on H-1B filings, I-9 or E-Verify hygiene, site-visit playbooks, and export-control screenings can be utilized for regulatory compliance. Centralizing documentation, including detailed job descriptions, minimum requirements, recruitment records, expert letters, and project scopes mapped to visas, may streamline the process. A startup, for example, may be able to standardize PERM recruitment templates and maintain versioned role matrices tied to standard occupational classification (SOC) codes and prevailing wages.

- **Expert immigration counsel and operational process.** Retaining expert immigration counsel and operationalizing processes may strengthen outcomes. Engaging counsel experienced in deep-tech O-1, EB-1A, NIW, and export controls and establishing service level agreements, checklists, and dashboards for case stages, may also improve efficiency. Training HR and project leads on criteria mapping, such as O-1 evidentiary prongs and reference letter best practices, may further support successful applications. A quantum consortium can use a panel of firms, with one dedicated to J-1 exchanges and another to EB-1 litigation. In addition, retaining counsel who understand the intersection between immigration and other areas of law, such as export control, can be essential.

- **Advocating for policy improvements.** Advocacy and collaboration for policy improvements shape a favorable immigration environment. Participation in coalitions such as the Security Industry Association and Center for Strategic and International Studies task forces, and the Quantum Economic Development Consortium (QED-C) could promote STEM green card reforms, cap relief, and NIW clarity. Providing data-driven comments on DHS and Department of Labor rulemakings and briefing congressional staff on quantum talent bottlenecks may influence policy. For example, an industry group can submit comments supporting streamlined O-1 criteria guidance for scientists and cap-exempt H-1B expansion for research and development.

- **Supporting international hires.** Integrating, supporting, and retaining international hires may warrant a holistic approach. Offering relocation assistance, spousal support, and awareness of dependent work options, such as L-2 spousal work authorization and H-4 EAD post-I-140 approval, may ease transitions. Providing mentorship, publication, and IP policies compatible with immigration goals and clear promotion paths could foster retention. For instance, a lab can pair new hires with mentors for grant writing and conference visibility in an attempt to strengthen O-1 and EB-1 profiles while possibly improving retention.

- **Aligning immigration with export control and security requirements.** Aligning immigration with export control and security requirements remains crucial to the quantum sector. Mapping roles to EAR or ITAR and deemed-export risks, implementing Technology Control Plans and facility-access zoning, and pre-screening candidates for restricted party concerns are steps for companies to strongly consider. Assessing CFIUS and research security implications for cross-border collaborations can protect sensitive work. For example, a quantum sensing program can segregate controlled design files, which allows foreign nationals to work on modular subprojects cleared under a Technology Control Plan.

- **Academic, government, and industry partnerships.** Building academic, government, and industry partnerships may expand access to talent and resources. Utilizing J-1 visas for visiting scholars and postdocs, coordinating with university sponsors for seamless transfers and extensions, and leveraging national lab collaborations, SBIR or STTR, and CHIPS, NSF, or DOE programs provide cap-exempt positions and shared talent. For example, a startup can co-host a J-1 research scholar with a university quantum center, then transition the scholar to a cap-exempt H-1B via the university and a concurrent H-1B with the startup.

Additional tactics could include considering remote-first or near-shore hubs to bridge urgent needs while U.S. filings proceed and maintaining immigration key performance indicators such as cycle times, approval rates, and retention outcomes to guide policy engagement and budgeting. By taking the above into consideration, the quantum industry can secure the talent necessary to maintain its leadership and drive future breakthroughs.

8 | Government Funding

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Government funding accelerates quantum innovation, but it imposes a dense, interlocking set of obligations across legal, technical, and operational domains. Quantum companies should treat compliance as a design requirement, embed it from program formation through performance and closeout, and protect both the science and the organization. Handled proactively, public funding serves as non-dilutive capital plus a path to validation, partnerships, and procurement. The payoff is faster execution, preserved rights, and a durable edge in a strategically vital field.

The U.S. government drives quantum innovation through two main levers: procurement and financial assistance. Procurement is the mechanism through which the government acquires technologies and services for defense, intelligence, research, and critical infrastructure. Financial assistance—including grants, cooperative agreements, Other Transaction Agreements (OTAs), Small Business Innovation Research (SBIR)/Small Business Technology Transfer (STTR) funding, Cooperative Research and Development Agreements (CRADAs), and Broad Agency Announcements (BAAs)—funds basic research, workforce and facilities, testbeds, and early commercialization. The U.S. Department of Energy (DOE), the National Science Foundation (NSF), the National Institute of Standards and technology (NIST), the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Activity (IARPA), the Department of Defense (DOD) and military services, guided by the National Quantum Initiative (NQI) and annual appropriations, use these tools to de-risk science, accelerate maturation across technology readiness levels (TRL), and signal national priorities.

Public funding comes with obligations that shape intellectual property (IP) and data rights, publication and reporting, cost allowability and audit, cybersecurity and controlled unclassified information (CUI) protection, export controls, foreign personnel and foreign influence disclosures, domestic sourcing and manufacturing, security clearances and foreign ownership, control, or influence (FOCI) mitigation, and downstream use restrictions. These awards also impose practical requirements such as milestone tracking, data management, reproducibility, and safety.

For startups, labs, and universities, the impact of public funding can be transformative, provided that teams embed compliance from the outset through governance, contracting processes, intellectual property (IP) strategy, secure enclaves, and supply chain planning rather than adding it later.

Key takeaways

- The governing instrument shapes the rules: grants, cooperative agreements, contracts, and other mechanisms impose different IP, data rights, and compliance contours. In quantum's interdisciplinary and international environment, spanning hardware, materials, firmware, control software, cloud access, and specialized supply chains, instrument choice carries outsized impact.
- Teams achieve success with early strategy and disciplined execution across the award lifecycle. Teams define publication and IP commitments under Bayh-Dole and agency clauses, flow down agreement requirements to collaborators and vendors, determine export jurisdiction and classification under Export Administration regulations (EAR) and International Traffic in Arms Regulations (ITAR), protect controlled data and controlled defense information (CDI)/controlled unclassified information (CUI) consistent with NIST standards, secure laboratories and cloud environments, implement data management and reproducibility plans, and meet milestones, reporting, audits, and business systems reviews.
- Organizations benefit from funding instrument-specific playbooks that map clauses to accountable owners, controls, evidence, and deadlines, enabling precise, consistent compliance at scale.

- **Ad hoc compliance carries potential for real downside impacts: loss of IP or data rights, clawbacks, suspension or debarment, export violations, reputational harm, weakened competitive position, and potentially civil and/or criminal penalties.**

8.1 KEY U.S. STATUTES THAT PROMOTE GOVERNMENT FUNDING OF THE QUANTUM INDUSTRY

8.1.1 U.S. Quantum Policy Landscape

The rapid growth of the U.S. quantum industry results, in part, from a strong legislative and policy framework that sets national priorities, coordinates interagency action, and sustains investment from research to commercialization. The National Quantum Initiative Act, the CHIPS and Science Act, and successive National Defense Authorization Acts anchor a whole-of-government approach that aligns federal agencies, academia, and industry. These statutes provide dedicated funding and strategic direction, advance workforce development, accelerate technology transfer, and safeguard critical quantum innovations. In addition, the National Institute for Standards and Technology (NIST), based at the US Department of Commerce, announced on September 24, 2025, that it is soliciting multi-million-dollar proposals to accelerate commercialization in critical industries such as advanced microelectronics and quantum technology. The announcement signaled the federal government's continued and growing interest in scaling the necessary domestic infrastructure needed for a robust quantum economy. By integrating economic, national security, and scientific objectives, they position the United States to lead the quantum ecosystem and translate breakthroughs into resilient industrial capacity.

8.1.2 Development: U.S. Policy Shift

Marking a notable shift in U.S. industrial policy, the federal government has recently taken direct equity stakes in major technology companies, most visibly in semiconductors. In August 2025, it acquired a 10 percent stake in Intel, replacing the traditional model of grants, loans, and tax incentives provided without ownership. The administration has signaled that it may take the same approach in other strategic sectors, including defense, AI, and critical minerals. While the United States took equity in failing private companies during the 2008 crisis, this move applies an industrial policy tool to healthy companies. The approach seeks to secure critical technologies, deliver a public return on investment, and bolster domestic manufacturing. It also raises important questions about state participation in private markets and may have implications for taxpayers, companies, and capital formation, including potential spillovers for quantum hardware, supply chains, and commercialization pathways.

8.2 AVAILABLE GOVERNMENT FUNDING AND RELATED PROGRAMS

8.2.1 U.S. Federal QIST Funding Landscape

U.S. government funding forms the backbone of the national QIST ecosystem, supporting foundational research, translational development, shared infrastructure, and workforce training. Building on the National Quantum Initiative and related authorities, federal agencies coordinate strategy and deploy a diverse portfolio of grants, centers, testbeds, consortia, and commercialization programs. Investments cover quantum computing, sensing and metrology, networking and communications, enabling materials and devices, and the software, benchmarking, and cybersecurity layers that integrate these systems.

8.2.2 Policy Coordination and Priorities

The NQI structure aligns federal activity in support of quantum information science and technology (QIST), and interagency bodies coordinate priorities, share roadmaps, and advise on long-term needs. These bodies partner with national laboratories, federally funded research and development centers (FFRDCs), universities, and industry to align funding with national objectives including scientific leadership, economic competitiveness, supply chain resilience, and national security. Current priorities include maturing hardware platforms, developing error correction and rigorous benchmarking, advancing quantum networking, securing cryptography in the post-quantum era, and expanding a specialized workforce.

8.2.3 Major Funding Agencies

- **Department of Defense (DOD).** DOD funds QIST for sensing, timing, navigation, secure communications, computing, and resilient architectures. Support ranges from basic research to advanced prototyping. Programs target fault-tolerant architectures, quantum error correction, benchmarking, mission-relevant algorithms, and quantum-enhanced sensing. Testing and evaluation, challenge problems, and formal metrics drive transition to deployable capabilities. DOD also uses SBIR funding and OTAs to promote industrial innovation.

- **Department of Energy (DOE).** DOE's Office of Science supports multi-institution efforts centered on national labs and universities, spanning quantum materials and devices, computing and algorithms, networking, and hardware-software co-design. DOE funds multi-year research centers and user facilities offering testbeds, fabrication, cryogenics, and photonics capabilities. It also advances quantum network infrastructure and demonstrations aligned with the national quantum internet vision, including metro-scale pilots and inter-lab links.

- **National Institute of Standards and Technology (NIST).** NIST leads in metrology, standards, and measurement science that underpin quantum devices and systems. Programs deliver benchmark measurements, reference materials, and standards for timing, sensing, and networking. Intramural research and joint institutes drive advances in trapped ions, superconducting circuits, photonics, and atom-based sensors. Public testbeds and measurement services support performance validation and interoperability. NIST also leads post-quantum cryptography standardization and technology transfer.

- **National Science Foundation (NSF).** NSF anchors academic discovery and talent development across QIST. Funding ranges from single-investigator awards to large centers focused on computing, sensing, and communications. NSF supports convergent research institutes, materials foundries, curriculum development, traineeships, and broadening-participation initiatives. Shared testbeds, software stacks, benchmarking, and verification efforts bridge basic science to usable platforms, with applications in chemistry, materials, optimization, and the physical and life sciences.

- **Additional civilian agencies and cross-cutting programs.** Other agencies fund quantum-relevant materials, devices, and networking research and development, strengthen standards and spectrum policy, and support mission-focused applications such as climate and environmental sensing, precision timing for critical infrastructure, and space-based experiments. SBIR and STTR programs across agencies catalyze startups and scale-ups in components, control electronics, cryogenics, advanced materials, software, and system integration.

8.2.4 Shared Infrastructure and Consortia

A growing emphasis on shared infrastructure lowers barriers to entry and speeds validation. National labs and universities operate open-access testbeds, cloud-access quantum processors, and network pilots that enable technology comparison, benchmarking, and co-design. User facilities provide superconducting, photonic, and atom-based fabrication, along with packaging, control, and cryogenic capabilities. Public-private consortia align federal funding with industry roadmaps to accelerate technology transition, develop supply chains, and shape standards.

8.2.5 Workforce Development

Workforce programs span undergraduate research, graduate traineeships, postdoctoral fellowships, and lab-based residencies. Interdisciplinary curricula integrate physics, electrical and materials engineering, computer science, and mathematics. Agencies fund educator training, curriculum resources, and partnerships with community colleges and minority-serving institutions to broaden participation and build regional capacity.

8.2.6 Translational and Security Investments

Translational programs bridge research to product through milestone-driven grants, cost-shared partnerships, and procurement-oriented pilots. Agencies support technology readiness assessment, benchmarking, and verification to reduce adoption risk. Parallel investments in cybersecurity and standards enable safe deployment, including post-quantum cryptography migration, quantum-safe networking, and secure interfaces between classical and quantum systems.

8.3 GOVERNMENT CONTRACTING FRAMEWORK FOR QUANTUM PROCUREMENT: FAR AND DFARS

Government procurement of quantum technologies operates within a dense set of federal statutes, regulations, and policies shaped by rapid technical advances and heightened national security concerns. The Federal Acquisition Regulation (FAR) serves as the baseline rulebook for executive agency acquisitions and sets uniform policies for government procurement of supplies and services, including quantum hardware, software, and research. The FAR governs competition and socioeconomic requirements, contract types, contractor responsibility, acquisition planning, contract administration, intellectual property, national security, and dispute resolution. Pursuant to an Executive Order issued in April 2025, the FAR will undergo a significant revision intended to return the FAR to its statutory roots, rewrite it in plain language, and remove most non-statutory rules.

For Department of Defense procurements, the Defense Federal Acquisition Regulation Supplement (DFARS) supplements the FAR with defense-specific requirements. DFARS governs contracts for goods and services with the DOD and governs procurement issues relating to cybersecurity, specialty metals, export controls, technical data rights, cost accounting, procurement integrity, industrial security, and supply chain risk management. It aligns with defense statutes, executive orders, and national security directives, and often imposes stricter standards for contractor qualifications and supply chain integrity.

Quantum contractors performing DOD-funded efforts must follow the FAR and DFARS, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Assistance Awards (Uniform Guidance) when applicable, along with any agency supplements tied to the specific funding instrument. They must also comply with export controls, domestic preference requirements such as the Buy American Act, intellectual property protections, and rigorous cybersecurity obligations for Controlled Unclassified Information and Controlled Defense Information. Given the dual-use nature and strategic significance of quantum technologies, procurements often involve enhanced scrutiny, classified contracting procedures, and elevated supply chain risk measures. Success in this environment may depend on early identification of applicable obligations, integration of compliance into program management, and close coordination with contracting officers as technical standards and policies in the quantum sector evolve.

Establishment of Responsibility Criteria

Under the FAR, contracting officers may award a federal contract only if they affirmatively determine the contractor is responsible. Responsibility depends on integrity, technical competence, and sufficient financial and organizational resources to perform. Contracting officers assess a contractor's financial stability, schedule compliance, past performance, ethics, organizational adequacy, accounting systems, and operational controls by conducting past performance reviews, financial and technical evaluations, facility checks, and exclusion database verification. For quantum programs, agencies typically expect contractors to show specialized quantum expertise, mature cybersecurity and supply chain risk management, export control compliance, and capabilities to protect controlled unclassified and classified information. Demonstrating responsibility in this context may advance both award eligibility and the security of U.S. quantum research and supply chains.

System for Award Management (SAM)

Entities that seek to compete for or receive federal contracts or assistance involving quantum technologies must register in SAM and keep their registration active. SAM verifies an entity's legal existence, eligibility, representations and certifications, and exclusion status, and it assigns the Unique Entity Identifier (UEID) used for offers, awards, and payment. Most actions also require a Commercial and Government Entity (CAGE) code associated with a specific facility, and agencies commonly extend these requirements to subcontractors and lower-tier assistance participants. SAM also serves as the primary portal that notifies the public of federal opportunities for contracts and financial assistance awards. Quantum contractors may want to consider running targeted searches for "quantum computing," "quantum sensing," or "quantum communications," and reviewing statements of work, proposal instructions, deadlines, points of contact, and applicable FAR or DFARS clauses. Contractors may also consider giving particular attention to security classification guidance, export control restrictions, performance standards, and any additional eligibility or compliance conditions. By saving searches and enabling alerts, contractors can monitor opportunities proactively, which can aid in responding in time to high-value quantum opportunities. Although direct agency outreach can support capture efforts, FAR and other rules can directly or indirectly limit funding, timing, and permissible communications after an agency issues a solicitation or during evaluations.

8.4 GOVERNMENT CONTRACTS AND ASSISTANCE AGREEMENTS

8.4.1 Government Contract Types for Procurement and Federal Financial Assistance

The U.S. government employs multiple funding instruments to accelerate quantum research and development, scale manufacturing, and enable commercialization. Agencies deploy grants, cooperative agreements, procurement contracts, OTAs, and lab partnerships such as CRADAs to resource researchers, startups, and industrial partners. Complementary programs provide testbed access, infrastructure support, workforce training, prizes, and technology transfer assistance to reduce barriers to entry and speed the transition from lab to market. Selecting the correct instrument can be of critical importance because it drives cost, schedule, performance risk, data rights, security obligations, and compliance expectations, especially where controlled technical information, classified work, or evolving performance metrics are involved.

The principal instruments for quantum programs include agreements listed below. Availability and terms vary by statute and agency. The solicitation and the FAR or agency supplements can be consulted for details.

- **Cooperative Agreement.** Assistance for a public purpose with substantial agency involvement in performance or management. Appropriate when collaboration, technical input, and joint decision-making are necessary. Governed by the Uniform Guidance.
- **Cooperative Research and Development Agreement (CRADA).** Collaboration between federal laboratories and non-federal partners using government facilities, personnel, and resources, with or without reimbursement. May be effective for pre-commercial quantum research and development and technology transfer.
- **Defense Production Act Agreement (DPA).** Authority to expand or secure domestic industrial capacity essential to national defense. Supports incentives, purchase commitments, and supply chain strengthening for critical quantum technologies.
- **Grant.** Assistance for a public purpose without acquiring goods or services for government use. Governed by the Uniform Guidance and focused on program objectives, reporting, and allowable costs rather than procurement deliverables.
- **Other Transaction Agreement (OTA).** Flexible, non-FAR instrument for research and development, and prototype contracts with tailored IP, cost sharing, and deliverables. Designed to attract non-traditional performers and accelerate innovation in defense and civil missions.

- **Procurement Contract.** FAR- and DFARS-governed acquisition of goods or services for government use, including research services. Establishes enforceable obligations on price, performance, and delivery. Primary vehicle for defined end products, capabilities or services.

- **Technology Investment Agreement (TIA).** DOD assistance instrument for research and development with strong commercial potential when traditional instruments are unsuitable. Enables flexible cost sharing, IP, and management to promote transition.

8.4.2 Contract Deliverables

Clear, enforceable deliverables are central to successful quantum contracts and assistance awards. Deliverables are the goods, services, data, and other outputs the recipient must provide under the Statement of Work, Performance Work Statement, or Statement of Objectives. Deliverables may include hardware, prototypes, subsystems, software, firmware, algorithm documentation, source code, test plans and reports, datasets, training materials, manufacturing readiness artifacts, intellectual property disclosures, and interim or final technical reports, and each category is subject to specific data rights and security clauses.

All deliverables must meet the specifications, quality standards, formats, and schedules in the agreement. The government typically accepts deliverables before it authorizes payment. Failure to deliver on time or to specification can constitute a breach and may trigger remedies including withholding, termination for default, or other contractual actions. In the quantum context, parties can define milestones, performance metrics, data rights, and cybersecurity and export controls with precision to manage risk, ensure compliance, and protect the government's interests while enabling technology transition.

In advanced R&D and technology contracts, such as those involving quantum science, deliverables often include milestone demonstrations, source code, algorithm documentation, IP disclosures, and interim or final technical reports, and each is governed by specific data rights and security clauses. All deliverables are to conform to the specifications, quality standards, formats, and delivery schedules established in the contract, and the government typically requires formal acceptance before it authorizes payment. Failure to deliver the required output on time or in accordance with contract requirements may constitute a breach, which can expose the contractor to remedies such as withholding payment, termination for default, or other contractual and legal consequences. Clear, detailed, and enforceable deliverable requirements can help ensure successful project outcomes and protect the government's interest in quantum technology acquisitions.

8.5 INFORMATION RELEASE RESTRICTIONS

U.S. government contracts and assistance agreements restrict the release or dissemination of information developed under an award to protect sensitive, proprietary, and national security-critical data, while preserving the government's rights to use and control such information for mission needs. These restrictions arise from statutes, the Uniform Guidance, FAR and DFARS clauses, agency policies, and export control laws such as ITAR and EAR.

Restricted information includes Controlled Unclassified Information, export-controlled technical data, classified information, proprietary and business-sensitive materials, and any other information that the contract designates for publication or release controls. Applicable law requires contractors to apply the required legends or distribution statements to all deliverables, and each category carries specific marking, handling, and access requirements. It also requires contractors to ensure that only authorized personnel have access and that any dissemination complies with applicable laws and award terms.

Agencies such as DOD, DOE, and NASA commonly require contractors to submit proposed publications, presentations, and public communications for pre-release review and approval to prevent inadvertent disclosure. Quantum programs often impose tighter controls given the national security implications of algorithms, cryptographic methods, device architectures, and enabling hardware. Export control laws and special access rules may restrict even unclassified R&D output due to the dual-use nature and strategic value of quantum capabilities. Contracts in this field may include enhanced clauses or tailored instructions governing handling, marking, and dissemination across all project information and deliverables, and contractors must maintain rigorous compliance protocols to prevent unauthorized disclosure.

8.6 RESEARCH SECURITY FOR QUANTUM R&D

8.6.1 ComplianceCan Be a Competitive Advantage

Organizations that pursue government funding may choose to look at research security as both a compliance requirement and a strategic enabler. The collaborative, cross-border, and fast-iterating nature of quantum R&D heightens exposure to export controls, data rights pitfalls, cybersecurity obligations, and research integrity risks. Effective programs begin at proposal development, strengthen during award and performance, and continue through IP stewardship and publication practices after project closeout.

Research security is the set of governance, legal, technical, and operational controls that protect sensitive information, comply with applicable regulations, and preserve research integrity. An organization's approach must be tailored to the sponsor (DOD, DOE, NIH, NSF, NASA, etc.), award type (grant, cooperative agreement, contract), data type (e.g., CUI, export controlled, human subjects, proprietary), and specific clauses incorporated by reference.

8.6.2 Lifecycle Framework

This framework applies across agencies and spans the period from proposal through execution for government-funded quantum R&D. It focuses on legal and contracting hooks, data classification, technical and administrative controls, and common traps that undermine compliance and commercialization.

- **Proposal stage: secure and strategic submissions.** Quantum proposals are sensitive technical artifacts, not marketing collateral. Proposals often contain controlled details and proprietary know-how for superconducting, trapped-ion, photonic, or QKD systems and for enabling infrastructure such as dilution refrigeration and control stacks. Items to consider in this respect: Default to data minimization, supply only what sponsors require, apply appropriate proprietary legends, and place deeper disclosures in secure annexes where allowed. Apply the proprietary legends in all proposals consistently using language in accordance with regulatory guidance, especially in SBIR and STTR, to preserve trade secrets and data rights.

  It can also be important to prioritize export control screening. High-level architectures may be shareable, but coherence tuning methods, cryogenic wiring, fabrication parameters, calibration waveforms, and similar content may be controlled. If inclusion is necessary, the control regimes can be identified, then the material can be marked, and appropriate restrictions to access can be utilized to permit authorized personnel only within controlled systems. It is also important to have accurate disclosures of outside affiliations and foreign support, which sponsors are scrutinizing more closely.

- **Postaward framework and compliance anchors.** Obligations depend on the sponsor, award instrument, and incorporated clauses. Quantum awardees often handle Controlled Unclassified Information. For example, DOD instruments may require safeguarding and cyber incident reporting aligned with NIST SP 800-171, including encryption with FIPS-validated modules, multifactor authentication, configuration baselines, centralized logging, a System Security Plan, and Plans of Action and Milestones. Other agencies impose analogous requirements with different terminology.

  Export controls can be addressed through a Technology Control Plan that governs personnel access, lab spaces, and digital repositories. The goal is not isolation, but disciplined routing of sensitive technical data, such as control-pulse source code, firmware, proprietary error-mitigation models, and high-resolution device characterizations, into role-based, auditable enclaves.

- **Data classification and handling.** Some work may qualify as fundamental research, which preserves open publication and international participation, but the status remains fragile. Publication or participation restrictions can negate it, and even open projects may contain nonpublic elements such as foundry recipes, process design kits, or sponsor-furnished information. Environments where CUI or export-controlled data is present can be segregated to avoid co-mingling with open research. A Technology Control Plan could be used to document access approvals, physical protections, and configuration controls. While human-subject data is rare in quantum, personally identifiable information can surface in collaboration platforms and requires appropriate protection.

- **Technical infrastructure and cloud controls.** Quantum labs blend IT and operational technology (OT) across cryogenic test stands, ion-trap systems, optical benches, and integrated control stacks that span lab networks and cloud orchestration. Consider cloud services that can be configured to meet applicable controls, enforce encryption at rest and in transit, and integrate with enterprise identity and logging. Also consider the segregation of environments that host sensitive source code, device characterization datasets, and sponsor-provided models from general lab systems. Consider encrypting and regularly test backups. Cloud platforms can simplify evidence of control coverage, but configuration discipline and documented change controls determine success.

- **Research integrity and foreign influence.** Sponsors expect robust protections against research integrity failures and foreign influence, especially in quantum programs. Conflict-of-interest and conflict-of-commitment disclosures can be centralized so that faculty, staff, and key personnel record external appointments, financial interests, and foreign support per sponsor policy. Oversight of publications may also be warranted to enable timely dissemination while meeting export control reviews, sponsor approvals, and IP protection.

  Quantum projects often straddle open-source science and proprietary information and technology development. Using a pre-publication review may prevent release of controlled details and to preserve patent rights. Delivering role-based, practical training that translates requirements into lab practice, including how to mark cryostat data, where to store error-correction benchmarks, how to grant time-bounded least-privilege access, and how to spot and escalate exfiltration indicators, can greatly facilitate the process.

- **Supply chain, subcontracts, and collaboration risk.** Supply chains and collaborations drive quantum progress and risk. Including flow down-required cybersecurity, data rights, export control, and incident reporting clauses into subcontracts and consulting agreements can facilitate compliance with prime agreement obligations. Partners can be assessed beyond credentials by testing their data protection posture, cloud configurations, incident readiness, and discipline with markings and publication controls. Design kits, layouts, firmware, and measurement data can be shared inside provisioned, logged workspaces that enforce least-privilege access and prevent uncontrolled onward sharing. Clear incident roles and timelines can be maintained across primes and subs, recognizing that reporting windows can be short.

- **Incident response for information and operational technology.** Incident response plans can cover software repositories, lab networks, and instrument controllers. Such plans can define indicators of compromise, immediate containment that preserves forensic artifacts, required notifications and timelines, and leadership roles for technical triage and sponsor communications. After-action reviews can be conducted that update the System Security Plan, Technology Control Plan, training, and access controls. Because collaborations are common, cross-organizational playbooks for quarantining shared datasets and revoking credentials while limiting disruption can be included.

- **Documentation as a strategic asset.** Documentation signals responsibility, compliance, and readiness and accelerates awards. A current System Security Plan shows design and ownership of controls. A Technology Control Plan bounds and audits export-controlled work. A Data Management and Sharing Plan clarifies what will be public and what will be restricted. Incident response plans demonstrate preparedness. Publication and communications plans align scientific goals with compliance. Access control matrices and training records show that policy reaches practice. Together, these artifacts help organizations scale from pilots to mission-critical programs.

- **Small businesses and startups.** Startups face enterprise-grade requirements with limited resources. The answer may be disciplined scope, right-sized secure cloud environments, and precise documentation of control coverage. SBIR and STTR programs reward careful data rights markings and deliverable handling, which protect advantage as markets adopt quantum capabilities. As quantum computing intersects with cybersecurity, it may help to keep a clear boundary between cryptographic research and operational security. Sponsors expect innovation in the former and standards-based execution in the latter.

Research security in quantum may amount to a design problem. It relies on intentional choices about architecture, access, and accountability that reflect the sensitivity and dual-use nature of the technology. Done well, it enables trust. Teams can publish, partner, and scale while meeting sponsor obligations, protecting IP, and safeguarding integrity. In a field where laboratory breakthroughs quickly translate into strategic capabilities, that trust is as critical as any qubit count or coherence time.

CMMC 2.0 for All DOD Contracts Begins November 10, 2025

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's program that verifies contractors safeguard the government's sensitive but unclassified information. It applies whenever a contractor's systems handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), with a limited carve-out for contracts solely for commercially available off-the-shelf items. The program formalizes long-standing obligations in FAR and DFARS by requiring assessed, attestable compliance and by flowing those requirements down through the supply chain to subcontractors that handle the prime's data.

CMMC 2.0 rollout: The DOD finalized the CMMC program rule on October 15, 2024, and effective on November 10, 2025, enabling contracting officers to specify the required level and assessment type in solicitations and contracts and to verify status in the Supplier Performance Risk System.

- **Nov 10, 2025:** CMMC clauses start appearing in solicitations and contracts; Phase 1 begins.
- **2026–2027:** Contracting officers increasingly require Level 2 third-party certifications and introduce Level 3 where warranted.
- **By 2028:** DOD includes CMMC in all applicable contracts (absent authorized government waivers for particular contracts or use of only commercial-off-the-shelf product exemption (COTS)).

Levels and assessment: CMMC 2.0 aligns to NIST and uses three levels keyed to the data at issue. Level 1 (Foundational) covers FCI with 15 basic safeguards and requires an annual self-assessment and executive affirmation. Level 2 (Advanced) covers CUI by implementing all 110 requirements of NIST SP 800-171; most acquisitions require a third-party assessment every three years, while some lower-risk efforts allow self-assessment; in all cases organizations must provide an annual affirmation. Level 3 (Expert) applies to select highest-risk CUI environments by adding 24 enhanced requirements from NIST SP 800-172 on top of Level 2, with government-led assessments. Limited Plans of Action and Milestones can support a short, conditional status, but organizations must fully implement priority controls to maintain eligibility.

Subcontractors and flow down: Primes must flow down the applicable CMMC clause whenever a subcontractor will process, store, or transmit FCI/CUI, and must verify the subcontractor's current CMMC status at the appropriate level before award. Primes may need to consider enclaving and scoping to minimize CUI exposure across the supply chain.

A practical consideration: For industry, the practical path may include determining whether your current or targeted work involves FCI or CUI; scoping the systems, assets, and vendors that will process that data; performing a gap analysis against the applicable controls; update the system security plan and artifacts; remediate deficiencies; and, where required, schedule a third-party or government assessment with enough lead time to account for backlogs. Primes may need to narrow the footprint of CUI across their supply chains through enclaves and careful scoping, confirm subcontractor status before award, and maintain continuous monitoring thereafter. Organizations that move early may reduce award risk as clauses proliferate and also strengthen security and resilience across their operations, which is the point of the regime and the foundation for long-term competitiveness in the defense industrial base.

8.7 MANAGEMENT OF DISPOSITION OF GOVERNMENT PROPERTY

Government contracts for quantum R&D routinely include detailed requirements for Government-Furnished Property and Government-Owned Property. In this sector, Government-Furnished Property often includes specialized test equipment, cryogenic systems, dilution refrigerators, quantum processors, quantum measurement devices, and related fixtures. Government-Owned Property includes property acquired or fabricated under a government contract, with title vesting in the government even if items remain at the contractor's site.

Contractors can consider maintaining a compliant property management system under the FAR and, where applicable, DFARS. At minimum, such a system documents receipt, tagging, inspection, inventory, use, maintenance, calibration, software or firmware version control, and protection. Government-Furnished Property is inspected upon receipt, labeled, and recorded in inventory. Contractors may use government property only for authorized contract purposes unless the Contracting Officer approves otherwise in writing. Contractors are required under applicable law to safeguard all government property against loss, theft, damage, or destruction and promptly report any incident to the Contracting Officer with sufficient detail to support investigation and resolution.

When government property is no longer required, the contractor notifies the Contracting Officer and requests disposition instructions. Disposition may include return to the government, transfer to another contract, sale or scrap with written authorization, or abandonment in limited cases. Proceeds from authorized sales or scrap are typically credited to the contract or are remitted to the U.S. Treasury as specified in the contract. Similar requirements may apply to financial assistance under the Uniform Guidance.

Quantum programs often require heightened controls given the dual-use nature and sensitivity of equipment and materials. Items such as superconducting chips, cold-atom systems, dilution refrigerators, and quantum control hardware may be subject to export controls, classification, or foreign national access restrictions. Secure storage, restricted laboratory access, chain-of-custody controls, and rigorous serialized tracking are essential. Calibration data, embedded software, FPGA bitstreams, control sequences, and technical documentation associated with Government-Furnished Property may constitute Controlled Unclassified Information and require proper marking, handling, and safeguarding. Effective property management supports regulatory compliance, protects national security, and preserves research integrity.

8.8 REQUIRED ACTIONS TO PROTECT GOVERNMENT INTERESTS

U.S. government contracts define contractual and procedural obligations to protect legal rights, operational needs, and national security throughout performance. The FAR, DFARS, Uniform Guidance, and agency policies ground these obligations, and program-specific clauses often tailor them. In quantum programs, agencies and contractors focus on intellectual property, information security, supply chain integrity, and performance controls to preserve government rights in deliverables, prevent unauthorized disclosure or misuse, and maintain agility to address evolving mission risks. Clear contract language that articulates these requirements supports compliance, audit readiness, and risk management across the lifecycle.

The following required actions commonly apply to government-funded quantum work, guiding execution and oversight. Where applicable, the parties should reference controlling regulations and agency directives and specify how each applies in the agreement.

8.8.1 Key Required Actions

- **Protecting intellectual property rights.** Contractors disclose subject inventions made during performance, elect titles within required timeframes, and file patent applications with the required government rights notices. They mark technical data delivered with limited or restricted rights to prevent the government from inadvertently acquiring unlimited rights. Sound IP management preserves government interests and enables appropriate commercial development.

- **Safeguarding controlled and classified information.** Contractors implement NIST-based controls for FCI and CUI, comply with DFARS cyber requirements for covered defense information (CDI), and follow the National Industrial Security Program Operating Manual (NISPOM) for classified work. They restrict access, prevent unauthorized disclosure, and report and remediate incidents rapidly within specified timelines.

- **Maintaining supply chain integrity.** Contractors avoid prohibited sources, including entities on the U.S. Bureau of Industry and Security (BIS) restricted lists, Federal Acquisition Supply Chain Security Act (FASCSA) orders, and providers of covered telecommunications or prohibited software. They maintain traceability for critical components, including quantum processors, control electronics, and cryogenic subsystems. FAR and DFARS prescribe additional source restrictions and reporting requirements.

- **Ensure performance continuity.** Contractors sustain adequate financial, technical, and staffing resources and maintain contingency plans to meet milestones. During mergers, divestitures, or reorganizations, contractors take prescribed actions to avoid performance disruption and to protect government interests.

- **Meet reporting and certification requirements.** Contractors submit timely and accurate technical, financial, and progress reports and certify compliance with applicable laws and regulations, including domestic preference rules such as the Buy American Act, to enable oversight and accountability.

- **Cooperate with audits, inspections, and reviews.** Contractors provide access to records, facilities, systems, and personnel for verification activities and promptly correct deficiencies identified by the Contracting Officer or Inspector General.

8.8.2 Additional Possible Safeguards for Quantum Contracts:

- **Exporting control compliance.** Contractors prevent unauthorized exports and deemed exports of quantum hardware, software, algorithms, and know-how, and they ensure compliance with ITAR, EAR, and related regimes.

- **Enhancing security measures.** Given the dual-use and sensitive nature of quantum R&D, contractors apply heightened controls to protect information that agencies may classify or that foreign actors may target, including prepublication review and strict need-to-know controls.

- **Preservation of commercial value.** Contractors manage background and foreground IP and data rights to balance mission needs with commercialization potential, maximizing public benefit while supporting private-sector innovation.

8.8.3 Safeguarding Controlled and Classified Information

Safeguarding CUI and CDI is central to quantum contracts. NIST frameworks require contractors to implement comprehensive measures for government-provided or contractor-generated sensitive data, including unclassified Controlled Defense Information. CUI and CDI commonly include export-controlled technical data, proprietary performance specifications, and sensitive research results. Contractors must implement baseline measures, including role-based access controls, system audit logging, multi-factor authentication for privileged access, encryption at rest and in transit, and rapid incident reporting and containment procedures. In quantum projects, CUI and CDI often encompass quantum encryption methods, device calibration data, cryogenic and RF designs, fabrication process details, and sensor architectures with defense or dual-use applications. Contract provisions typically require contractors to meet specified implementation timelines, assessment standards, and reporting channels.

8.8.4 Domestic and American Preference Requirements

Federal contracts frequently require or prefer U.S.-origin goods or select foreign origin materials and services under domestic preference frameworks such as the Buy American Act and the Trade Agreements Act, subject to exceptions and waivers. Contractors must certify compliance, meet domestic manufacturing and content thresholds, and retain documentation supporting country-of-origin determinations. For quantum programs, domestic preference often applies to key items such

as cryogenic systems, superconducting materials, precision instrumentation, quantum processors and control electronics, shielding and specialty metals, and secure communications equipment. Given global supply chain difficulties, contractors may choose to map sources early and verify origin. Where U.S. supply is limited, contractors may pursue approved exceptions or work with government stakeholders on industrial base support mechanisms to develop and qualify domestic sources. Many contracts also require U.S. manufacturing for products that embody government-funded technology.

8.8.5 Required Actions for Foreign Access, Involvement, and Control

Foreign access, involvement, and control receive heightened scrutiny in quantum programs due to strategic and dual-use considerations. Beyond baseline ITAR, EAR, and NISPOM compliance, contracts may impose additional restrictions such as requiring prior written approval for foreign involvement, limiting foreign national participation, and mandating disclosure of planned or actual foreign roles. Contracts may require facility and personnel vetting, including Foreign Ownership, Control, or Influence (FOCI) mitigation when facility clearances are implicated, via instruments such as Special Security Agreements, Proxy Agreements, or solicitation requirements. Agencies often apply supplemental controls to quantum hardware, control software, and algorithms and may require additional review by the Department of Commerce or NSA, even in unclassified efforts.

Participation by foreign entities and individuals is not categorically barred, but such participation must be expressly permitted or approved by the Contracting Officer and must comply with export controls and security requirements. Contractors may choose to carefully vet subcontracts to foreign firms, obtain approvals where required, and strictly handle controlled items and data under appropriate licensing. Contractors may also choose to limit engagement of foreign nationals to non-controlled work or cover such engagement with export authorization, supported by Technology Control Plans that govern physical, digital, and procedural safeguards.

Given the classification of many quantum technologies as emerging critical technologies, agencies may further limit foreign participation in sensitive tasks and restrict offshore fabrication of quantum devices due to supply chain security and domestic sourcing rules. Contractors can maintain rigorous screening, disclosure, and control processes to protect government interests and sustain uninterrupted performance.

8.9 SBIR AND STTR: GOVERNMENT R&D FUNDING FOR SMALL BUSINESS

The United States uses the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs as core instruments to advance small-business R&D. For the quantum sector, these programs provide a competitive pathway from early research to commercialization of quantum computing, sensing, and communications technologies. (Note: The SBIR and STTR program authorities expired on September 30, 2025, but it is anticipated the authority will be renewed once the government shutdown ends.)

SBIR accepts quantum companies with 500 or fewer employees (including affiliates) and supports independent R&D. STTR requires a formal collaboration with a U.S. nonprofit research institution, such as a university or FFRDC, with mandated minimum workshare to ensure real technology transfer. Agencies fund SBIR and STTR as grants or contracts. Grants typically let investigators drive projects and suit foundational quantum research. Contracts prescribe requirements and align with defined mission needs. National Institutes of Health (NIH), NSF, and parts of DOE often award grants; DOD, Department of Homeland Security (DHS), NASA, parts of DOE, the Environmental Protection Agency (EPA), Department of Transportation (DOT), and Department of Commerce (DOC) frequently award contracts. Some agencies award both, depending on topic and program goals.

Eleven agencies offer SBIR opportunities: DOD, the Department of Health and Human Services (HHS) and NIH, DOE, NSF, NASA, DHS, the Department of Agriculture (USDA), DOC (NIST and NOAA), DOT, EPA, and the Department of Education (DOE). Five also run STTR: DOD, HHS and NIH, DOE, NASA, and NSF. Many agencies now tailor dedicated quantum topics to their missions. U.S. law requires agencies with sizable extramural R&D budgets to set aside funds for SBIR and STTR. These set-asides, along with evaluation criteria and phased award structures, create clear pathways for quantum firms. Agencies may issue Phase III awards as sole-source contracts (i.e. not competitively awarded) without further competition when the awards build on prior SBIR or STTR work, which enables faster transition and scaling.

For quantum startups, awards provide non-dilutive capital, technical validation, and credibility with investors and partners, while opening government and commercial markets. In short, SBIR and STTR pivotally move quantum innovations from lab to deployment and sustain U.S. leadership in quantum technologies.

Key Considerations: Government Funding for Quantum Technology

Securing and managing government funding in quantum could warrant disciplined planning, rigorous compliance, and proactive risk management. The following considerations help startups, universities, established companies, and investors maximize opportunities and protect core interests.

- **Building the right team.** Staff projects with experts in government contracts, compliance, cybersecurity, and classified work. Where gaps exist, it may be beneficial to retain advisors with federal funding and technology commercialization experience to avoid process errors and protect program eligibility.
- **Preparing early and staying organized.** It may be advantageous to begin applications, compliance plans, and internal controls well ahead of deadlines. Maintaining complete records, audit-ready documentation, and clear task ownership may enable timely responses to government inquiries.
- **Prioritizing security and compliance.** Mapping applicable requirements at the outset, including cybersecurity, facility clearances, personnel vetting, data handling, and reporting may also aid the process. Controls can also be embedded into workflows to help prevent delays, penalties, or disqualification.
- **Protecting intellectual property.** IP can be treated as a strategic asset. Conducting diligence and negotiating IP clauses, data rights, and publication terms before awards are actions that can also be considered. It may also be important to align contract terms with commercialization goals and academic obligations and implement internal IP controls.
- **Managing export controls and foreign investment.** Parties have found it important to identify export control classifications, end-use restrictions, and potential licensing needs early. Other considerations here include assessing foreign investor and collaborator implications, including national security reviews, and obtaining required approvals.
- **Engaging government stakeholders.** Early professional communication with program officers and contracting officials, including seeking clarification on requirements and leverage feedback to strengthen proposals and performance may be helpful.
- **Tracking regulatory change.** Monitoring updates to procurement rules, cybersecurity frameworks, export controls, and national security policies, and adjusting strategies and compliance programs as requirements evolve.
- **Using agency support resources.** There are training, webinars, templates, FAQs, and help desks that funding agencies offer to refine applications and strengthen compliance.

9 | Venture Capital

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Venture capital plays a central role in building quantum companies in computing, communications, and sensing, where long research and development cycles, high capital intensity, and specialized talent drive risk and financing needs. Early funding remains founder-friendly and milestone-driven, while later funding becomes larger, more structured, and designed to support scale and commercialization. Each stage marks an evolving risk profile and capital requirement.

This chapter provides foundational information to inform start-ups and investors about key considerations related to corporate formation decisions and investment structures that are suited to quantum's longer horizons, and governance and control rights that balance investor oversight with founder agility. It also demystifies economic terms for investments, tying valuation mechanics, dilution, and downside protections.

As with government funding, an early understanding helps teams to convert capital into durable advantage by structuring companies for scale, securing aligned partners, and preserving strategic flexibility while managing dilution, control, and execution risk intentionally.

Key takeaways:

- **For founders, anchor clarity of milestones and capital strategy in robust legal foundations. Structure fundraises to comply with securities laws; prioritize patent filings, trade secret management, and freedom-to-operate analyses to help build defensible positions; and negotiate commercial agreements carefully to try to allocate risk and preserve future flexibility. Cross-disciplinary teams can navigate both scientific and legal due diligence.**
- **For investors, match deep technical diligence with legal diligence. Investment documents may address governance, liquidation preferences, anti-dilution protections, and exit rights. Reinforce staging investments through tranched rounds tied to technical inflection points with clear contractual milestones. Investors may choose to evaluate regulatory risks, export controls, and the enforceability of IP rights in different jurisdictions. Realistic exit planning, whether through merger/acquisition, IPO, or secondary sales, may require careful attention to representations, warranties, and indemnities in transaction documents.**

9.1 CORPORATE FORMATION CONSIDERATIONS FOR QUANTUM FOUNDERS

There are many considerations that founders need to think through when starting their company. From ownership splits and role and responsibility assignments to entity selection choices, the details can be overwhelming and many of them need to be addressed before any papers are signed. The choices also often require alignment of all founding team members and while some (like the company name) are easy to change later, others (like equity splits) are harder to adjust without downstream taxes or other impacts. Founders should also keep in mind that investors expect that companies they fund will have certain attributes, like robust intellectual property ownership rules and vesting provisions in place.

Fortunately for both founders and investors, there are many defined norms for venture-backable high-tech companies, including quantum companies. The following covers a few of the most important concepts at a high level in an effort to orient founders to the most common considerations that should be addressed before (or shortly after) forming a tech startup company. Corporations (and use of corporate terms) are referred to in most of the sections, but the principles (and corollary terms) are often generally applicable to limited liability companies. For intellectual property and venture capital, see Chapter 3, "Intellectual Property Rights & Protections," Section 3.4.

Note that these topics are discussed at a very high level and it is certainly important to find a competent tech or startup attorney to advise on the meaning and application of these concepts for each unique situation. Further, there are many good resources within the startup ecosystem that can be leveraged, including knowledge bases and explanatory articles published by authoritative third parties like Carta (https://carta.com/learn) to learn more about unfamiliar terms and concepts and drill down before engaging a lawyer.

9.1.1 Entity Type

The choice for most founders and founding teams is whether to form a corporation or a limited liability company. The second consideration is where (meaning in what state or commonwealth) the entity should be formed in. A corporation is often the form required by third party investors, primarily for tax reasons; a corporation is itself taxed and, absent an exceptional circumstance, will not distribute profits to its investors (to avoid "double taxation"). However, a limited liability company will allocate profits and losses to investors, which can be a burden (or worse) for investors who would deal with uneven cash flow across a portfolio of investments.

Additionally, quantum companies that are formed as corporations are often also eligible to issue Qualified Small Business Stock (aka QSBS stock) under IRS Code Section 1202, which is a material incentive for investors in early-stage tech companies and also something founders want to explore for their own initial stock issuance. While corporations are subject to a substantial number of statutory requirements that define how they are formed and operate, those rules are generally viewed as a necessary tradeoff for investors who see those defined governance rules as beneficial protections and helpful standardization. In contrast, limited liability companies (LLCs) often have bespoke governing documents because the rules to form a limited liability company are so flexible. So, while LLCs can be very useful for experienced founders with unique situations or those that do not need to raise outside capital, the flexibility combined with the tax attributes of an LLC means investors often strongly prefer corporations.

In many cases, formation of a Delaware corporation is the appropriate choice for founders that want to position themselves to raise venture capital or dilutive funds from third parties. That does not mean a founder cannot incorporate or form their company in their primary state of residence, but the most common state of formation or incorporation is Delaware. Also, Delaware law is generally regarded as the gold standard of American corporate law and many states pattern their laws after the laws and principles of the Delaware business courts, called the Court of Chancery.

9.1.2 Roles and Responsibilities

Founders often wear many hats, but it is very important to define each founder's role on the team (and consequently, their responsibilities). In a corporation, which is the most popular "legal form" of a startup, there are three primary roles: a stockholder, a member of the Board of Directors (a.k.a. a "director") and an officer (e.g., the President, CEO, Secretary, Treasurer, CFO, COO, CTO, etc.).

- **Stockholders** own shares of stock in the company. Stockholders can be entities or individuals. For founders, their shares of company stock are usually granted at the time the company is incorporated, and their stock is often subject to vesting (more on that below). Stockholders can also acquire shares through the exercise of options, or their shares could be purchased in an investment round, among other alternatives.

- **Directors** are appointed by, and accountable to, the stockholders. Directors have fiduciary duties to the company, and, with few exceptions, they must act in the best interests of the stockholders in all respects. Under the laws of most states, the Board of Directors manages the strategic direction of the company and they need to approve the most important and material transactions (e.g., appointing officers, major contracts, financing transactions, equity grants, etc). Directors do not need to hold stock in the company but in most early-stage tech companies, the directors are founding team members, investors and, occasionally, industry experts. The size of the initial Board of Directors is usually between two and five members (and Board composition is discussed more in the financing sections below).

- **Officers** are appointed by and accountable to the Board of Directors. The officers manage the company's day-to-day operations. The CEO is almost always a member of the Board of Directors. It is important when appointing someone as an officer to define their specific job duties and what power or authority they have, if any, as officers are generally viewed as having the power to manage the company's operations and bind the company to third party contracts.

  When founders act on behalf of the company, it is important for them to consider (1) what role they're acting in and (2) if the action they're taking is something they are allowed to take on their own or if they need other approvals under their company's governing documents or applicable state law.

  It is also very important at the time of formation or incorporation for founders to agree amongst themselves how they'll manage the approval of material transactions, including whether certain types of transactions require a simple majority approval from the founders or whether all founders need to agree on a transaction before it is approved.

9.1.3 Founder Vesting

While founders often struggle to view their company as a separate and distinct entity from the founding team, it is important to note that sophisticated investors almost universally expect founders, as the first stockholders of the company, to subject their stock to a "vesting schedule."

The concept of "vesting" means that if someone stops providing services to the company, a portion of their stock would be forfeited back to the company. The "vesting schedule" defines the period of time over which the stockholder would need to provide services to fully earn their stock (meaning that some or all is released from the forfeiture restriction over time). The "standard" vesting schedule is a schedule where the shares of stock subject to vesting are earned over a period of four years, with 25% earned and released from vesting on the first anniversary of the commencement of the stockholder's services to the company and pro rata portions of the remaining stock vesting in equal installments over the remaining 36 months.

When a core founder or service provider (who may have a substantial amount of stock) leaves or is terminated, vesting can help re-balance any equity allocation that the departed individual has to reflect a shorter period of service to the company. The re-balancing is accomplished by that stockholder forfeiting some of their unearned (meaning unvested) equity back to the corporation and this avoids "dead" equity. "Dead equity" is a large block of stock held in an early-stage company by a non-active founder or service provider.

"Vesting" also usually requires the stockholder to file a Form 83(b) with the IRS. This is a critical topic to discuss with the company's startup attorney and CPA before any stock subject to vesting is granted/purchased as the Form 83(b) filing is time sensitive. Failure to comply with 83(b) rules is not just a stock recipient's issue—it can also be a major company tax issue.

Founders often think that vesting conditions only apply to later-stage hires—but it is actually very important to have early company hires subject to vesting, thereby ensuring that each core contributor/founder/early hire remains incentivized to help grow and develop the company over a multiyear horizon.

While vesting can apply to some of all of the shares owned by a stockholder, it is most common for vesting to apply to a stockholder's entire allotment of shares. Founders who have already devoted considerable time may negotiate partial credit toward the vesting schedule.

Other bespoke or unique terms, like milestone-based vesting or acceleration upon a change of control, can also be negotiated on a case-by-case basis. Those terms can differ depending on the stockholder's role with the company (e.g., a founder may have a different set of rules and vesting terms than a mid-level employee.)

9.1.4 Service Agreements

Founders and service providers execute comprehensive services agreements with standard terms. The standard terms include compensation details, services details and expectations, role and responsibility information, confidentiality and intellectual property assignment clauses and, if appropriate, restrictive covenants. Restrictive covenants, which are discussed more below, include non-solicitation provisions, conflict of interest restrictions and, if permitted under applicable law, non-compete restrictions. These agreements are often closely scrutinized by investors before any investment as part of their due diligence process.

If a service provider will receive a Form W-2 for their compensation, is paid through company payroll and engaged as an "employee," they would usually receive an offer letter detailing the terms above and the fact that employment is on an "at-will" basis. If a service provider will receive a 1099 form and be engaged as a "contractor," they would receive a consulting agreement or contractor agreement. Note that the title of a service provider's engagement agreement (and what you call them) does not determine whether someone is appropriately classified as an employee or a contractor. It is important to consult with your attorney about appropriate terms, and the material tax differences between these two types of service providers and the appropriate substantive classification of service providers.

9.1.5 Equity Incentive Plans

Most early-stage startup companies will adopt an equity incentive plan (EIP) and allocate a certain portion of the company's equity to the EIP in order to attract and retain talent. Using equity, whether it is a grant of restricted stock or options (each subject to vesting), can be particularly helpful where a company cannot afford to pay market rates of cash compensation to employees or contractors.

When allocating equity to the EIP, it is important to prepare a hiring plan and consider how much of the company (on a percentage basis) the company will need to achieve the hiring plan. The allocation is generally discussed on a percentage basis, e.g., 10% or 15%. Market data, including data published and tracked by Carta, can be helpful when benchmarking how much equity to give a certain type of service provider in a certain geography relative to the company's stage and type.

It is common for an EIP to authorize a variety of award types—Incentive Stock Options (ISOs), Non-Statutory Stock Options (NSOs), and restricted stock awards or grants (RSAs). The adoption of an EIP will almost always require both Board of Directors and stockholder approval, with subsequent management of the EIP done by the Board (or a committee of the Board for later stage companies). Increasing or decreasing the amount of stock reserved for issuance under the EIP generally requires stockholder approval as well.

Note that grants under an EIP—including the nuanced terms of the EIP and any option agreement or RSA—are subject to complex securities laws and tax rules and other limitations. While most sophisticated startup law firms have form agreements for the different types of EIPs, edits to the forms will require the assistance of a competent startup attorney, including usually an employee benefits and/or tax attorney. It is generally advisable to work with the company's startup attorney to develop a comprehensive approach to equity compensation and then generate standard forms for use by the company. Using that approach makes it easier to stick to appropriately drafted forms, which helps avoid ownership and other legal compliance issues or tax problems. Many of those issues are difficult and expensive problems to manage after they occur.

9.1.6 Restrictive Covenants

Managing turnover and retaining talent is critical for startup teams. Compensation and equity grants can be good retention tools, as can company culture, but investors expect that the company will also take certain steps to manage the downside risk of top talent departing (sometimes for a rival company).

Restrictive covenants include non-solicitation provisions (which restrict how someone can approach company employees, contractors and customers), conflict of interest provisions (to manage concurrent or post-engagement conflicts) and, occasionally, non-competition provisions that restrict how a service provider can compete with the company or engage in a competitive business after they leave the startup.

Well-drafted restrictive covenants preserve the company's core economic interests, including interests in its human capital and customer relationships. However, each state has different laws and requirements that will define what is and isn't permissible in restrictive covenants. These covenants must be calibrated to withstand judicial scrutiny, particularly in jurisdictions hostile to non-competes (e.g., California) so crafting these with the assistance of counsel is important. In some states, there are penalties for including certain restrictive covenants where those terms are prohibited by applicable law.

For founders and senior executives in jurisdictions that permit non-competes (e.g., Massachusetts, among others), reasonable restrictions typically span 6-12 months post-termination and cover competing activities within defined geographic and product markets. Non-solicitation covenants are quite common and should generally be included even where non-competes are disfavored. Most investors expect, and many standard investment documents require, startup companies to bind employees to non-solicitation and non-compete where permissible under applicable law.

Management of these covenants becomes easier if the company is vigilant about standardizing and complying with its onboarding and offboarding procedures, including executing separation agreements that re-acknowledge applicable restrictive covenants where the separated person owned equity, was key to the company's growth and/or materially participated in intellectual property creation.

9.2 INVESTMENT STRUCTURE AND SECURITIES

For founders, the choice of which security to issue to investors in exchange for new cash investment is highly fact-specific and is often driven by the stage of their business, their company's short-term needs, prospects and market trends. But in large part, the choice is between one of three options: (1) a Simple Agreement for Future Equity (a "SAFE"), (2) a convertible promissory note (a "convertible note") or (3) shares of stock in their company, often preferred stock. All are generally referred to as "securities" under applicable securities laws.

SAFEs are often only issued in pre-seed rounds as the first money into a startup company and they convert into shares of the issuing company's stock as part of the first preferred stock financing. Convertible notes are debt instruments that, like SAFEs, convert into shares of stock in a preferred stock financing. Unlike SAFEs or convertible notes where there is no company valuation implied in the financing, preferred stock financings require a valuation on the startup company and the company's issuance of a certain percentage of the company's stock at a specified valuation.

Beyond those very simple details, financings are very complex, oftentimes deceptively complex. A third-party investment transaction requires a founder to make a choice of how to structure an investment round (i.e., how much to raise and who to raise from), what security to issue to the investors, how to comply with applicable securities laws and what rights the company should provide to investors depending on how much they invest and when.

9.2.1 Type of Security (Preferred Stock vs. Convertible Notes vs. SAFEs)

SAFEs are non-debt securities that are treated as equity for tax purposes but are not actual shares of company stock. Only corporations can issue SAFEs. The definitive form of SAFE is published by YCombinator and is often used by early-stage pre-seed investors, angel investors and accelerators/incubators as a low-resolution, low-friction financing instrument. SAFEs convert into equity in the company's next equity financing and the stock issued to SAFE holders in such equity financing would have substantially the same rights and obligations as the new cash investors in that equity financing.

Convertible notes are interest-bearing debt instruments. They are not equity securities, and, like traditional debt, they have a maturity date. Convertible notes can be issued by pre-seed startups in small financing rounds or can be issued by later stage companies in "bridge" financing rounds (meaning they are issued between larger, usually equity, financing rounds and have shorter maturities). Convertible notes are often unsecured, and investors generally intend for the convertible note to convert into equity securities at the company's next equity financing. The terms and requirements of what constitutes a "next equity financing" are defined in the convertible note. Like SAFE holders when their SAFE converts, convertible noteholders will receive shares of stock in the next financing that have substantially the same rights and obligations as the new cash investors in that equity financing.

The issuance of shares of preferred stock in an equity financing is what most founders and investors think about when reference a "venture financing." An equity financing, often a "series" financing (e.g., a "Series A," Series B," etc.), is generally documented using the standard and open-sourced investment documents published and maintained by the National Venture Capital Association (NVCA).

The five core documents, while open-sourced and standard, are quite complex, which is why most equity financing transactions start with the negotiation of a term sheet between the lead investor(s) and the company. The term sheet often specifies the anticipated closing timeline and the core rights and terms of the preferred shares, including valuation, investment amount, share price, Board of Directors composition and other rights and preferences for the investors.

SAFE and convertible note financings are considerably simpler than traditional equity financings in which a company issues and sells preferred stock—though neither should be completed by a company without the advice of a competent startup lawyer.

Convertible note and SAFE financing transactions both involve fewer variables among the most common terms; there is less paperwork and the financing rounds are often substantially less expensive given their mechanics. However, those financing transactions are also often smaller (meaning the company receives less in aggregate investment) than equity financing transactions and with good advisors and attorneys, the complexity of an equity financing, especially one that uses the NVCA core documents, can be completed relatively quickly.

Many of these core terms that founders would see in equity financing transactions are discussed in greater detail in the sections below.

9.2.2 Representations and Warranties

In connection with investment transactions, the company is expected to provide certain statements of fact to induce the investors to complete their investment. These statements of fact, referred to as representations and warranties, are contractual statements made as of a particular point in time (often, the signing or closing of a transaction). They supplement—but do not replace and are not replaced by—legal due diligence that an investor may conduct before investing.

Though often used interchangeably, a "representation" is an assertion that a given fact is true, while a "warranty" is a promise that the fact will remain true or, if it proves false, that the party making the statement will indemnify the counterparty for resulting losses. Although the two concepts are frequently bundled together in practice, they serve slightly different purposes; representations provide a basis to rescind an investment (or worse) if representations were untrue when made, whereas warranties supply a contractual remedy—typically indemnification—if the statement turns out to be inaccurate post-closing. These nuances can often be managed with the assistance of the company's attorney but in any event, it is critical to make sure any company reads and understands both the representations and warranties that the company is making to investors in the core financing documents.

For founders, representations and warranties may not be top of mind like economic terms (valuation, etc.) but they are just as important as the core economic terms that otherwise take center stage in investments. Investors may note that the representations and warranties "allocate risk," which is true—should the investor or the company bear the burden of an undisclosed company issue? By compelling the company to disclose, among many other things, the state of its capitalization, intellectual-property ownership, legal compliance posture, and litigation exposure, representations and warranties give investors confidence that they understand precisely what they are investing into. And if the promises and statements made to the investors are false, the investor(s) may have recourse against the company.

Beyond facilitating transparency, representations and warranties play a crucial role in shaping the expectations and trust between parties in a transaction. Representations and warranties are usually paired with "disclosure schedules," disclosures of certain facts that qualify and supplement a specific representation or warranty (e.g., a list of a company's intellectual property would be included as a schedule, or a full capitalization table can be attached to "represent" as to the company's current ownership).

Representations and warranties should not be something founders are afraid of. With due care, such disclosures help ensure that all material facts about the company are clearly disclosed, reducing the risk of misunderstandings or disputes after the deal closes. Understanding how representations and warranties function—as both tools for disclosure and mechanisms for allocating risk—can help founders protect the company and foster smoother, more successful transactions when raising capital.

9.2.3 Securities Laws and Eligible Investors

Raising capital from investors, whether angel investors or venture funds, requires strict compliance with federal and state securities laws. These securities laws reinforce the general public policy that investors in early stage or high-growth companies should have the opportunity to be fully informed of all material facts about a prospective investment or they must be given access to such material facts and information in order to inform what is usually a risky investment.

Additionally, part of the most common path to comply with applicable securities laws is to raise money from "accredited investors" (as defined in Rule 501 or Regulation D, which is a specific section of the Securities Act of 1933). "Accredited investors" are individuals or entities meeting that meet specific criteria, including income or net worth thresholds or that meet certain unique sophistication requirements.

The securities laws that apply to the issuance of securities generally prohibit the "public offering" of "unregistered securities" so startups need to be mindful to find appropriate exemptions from "registration" and to make sure an issuance of securities constitutes a "private offering." While there are many different paths, including public equity crowdfunding options, the rules we discuss here are applicable to private financings and that path is by far the most common approach for early and mid-stage tech startup companies. But either way, all of these complex terms reinforce why it is important to have a competent startup attorney with experience navigating securities laws.

In addition to who you raise from and how, securities laws often require various federal and state-level filings with appropriate governmental authorities. The federal level filing is most commonly called a "Form D" and the state level requirements often trigger "blue sky" filings. Note that all of these filing requirements come with various pre- and post-closing activities and/or deadlines and many come with filing fees and costs.

Failure to comply with applicable securities laws can afford the startup company investors with various protections, including in some cases the right to rescind their investment. These investor protections make the rules important to review and abide by through careful advanced planning. Compliance with applicable laws also comes up in legal due diligence as part of subsequent financings and in company sale transactions.

9.3 GOVERNANCE AND CONTROL RIGHTS

Governance and control rights are core considerations when a startup is taking outside capital. When investors invest into a startup, they often expect a certain level of control over and visibility into the operations of the entity that they invested into. While the most significant of the controls (like participation in the company's governance through the ability to control a seat on the company's Board of Directors or veto rights over material company decisions) are reserved for lead investors that cut big checks, it is not uncommon for some or all investors to have information rights, rights of first refusal over founder stock transfers, and other material rights.

There are often few, if any, true governance and control rights in a SAFE financing—the standard YCombinator SAFE documents (https://www.ycombinator.com/documents/) do not provide such rights other than "pro rata rights" via the standard YCombinator published pro rata rights letter. But a lead investor that invests a substantial sum may ask for a "side letter" where additional rights are detailed. It is somewhat more likely to have investors ask for certain governance and control rights in a convertible note financing, and governance and control rights are a core part of standard preferred stock financing rounds, especially where the company is negotiating on NVCA form investment documents (https://nvca.org/model-legal-documents/).

Discussed below are some of the common rights; but founders looking to educate themselves further in advance of an equity financing should review the NVCA form documents. Those documents, especially the form of term sheet published by the NVCA, provide a good long form reference with helpful annotations. There are also many publicly available market studies that detail "standard terms" and startup company advisors can often be a helpful resource too.

Companies should work with their attorney to carefully consider the scope of the governance and control rights (i.e., what is being requested and are the requests "market" asks), who controls the rights (i.e., does each investor have their own veto rights or are the rights held by a group) and how long the rights survive (i.e., do they survive in perpetuity or do they subset based on the occurrence of certain events or failure of certain events, like an investor not investing further).

9.3.1 Board Composition

The structure, membership and size of the Board of Directors (Board) is a central element of corporate governance, balancing the interests of founders and investors. In almost all cases, a Board with an odd number of directors is best practice to avoid deadlocked (or tied) votes, regardless of the company's stage and industry. Board composition can be a difficult decision as many investors often see Board representation as a key lever to influence company direction. However, given the fact that directors owe fiduciary duties to the company, representation on a Board can cause conflicts for the founders and investors who are obligated to consider the company's best interests over their personal interests and/or their fund's interests.

Beyond having an odd number of directors on the Board, earlier stage companies (including companies after a first true financing) often have Boards with three to five directors to avoid cumbersome decision-making and scheduling hassles. Later stage companies (that are often post-Series B financing) can have larger Boards with up to seven members but having more than seven members is not common until the company is mature.

While many investors may ask for a Board seat, especially if the company has different lead investors across rounds, companies may ask early investors to allow their Board seat (and Board-level representation) to sunset and/or potentially shift into a Board "observer" role. A Board "observer" is a role with visibility into Board-level governance but without a formal vote (or any attendant fiduciary duties). Additionally, it is common for founders of early-stage companies to "control" the Board of their company through the power to appoint (or influence the appointment of) directors but that becomes less common as the company raises more money and matures.

As the NVCA forms note, there is no "market" for the specifics of Board composition—what is an appropriate Board composition is highly fact-specific. The precise allocation is often a matter of negotiation and generally reflects the relative bargaining power of the parties and the stage of the company.

Board composition is a core term that would be addressed in any equity financing term sheet and, as noted above, Board representation is standard in equity financing rounds but less common in convertible note rounds or SAFE rounds.

9.3.2 Voting Rights

For investors, voting rights are central to how they can manage early-stage investment risk. In an effort to protect their investments, investors frequently negotiate fulsome voting protections, which are often referred to as "protective provisions." The protective provisions are intended to require the company to seek and obtain the approval of a specified percentage of stockholders and/or investors (the "requisite stockholders") before taking a specific action or permitting an event to occur.

In negotiating the protective provisions, which can also be called "veto rights" for investors, there are two common issues that founders need to be mindful of. The first issue is the scope of the protective provisions—meaning what actions and events should require the approval of the requisite stockholders of the company before the company can take an action or permit the event to occur. Common protective provisions include the following core items: (a) the liquidation or sale of the company; (b) any amendments to the company's governing documents (e.g., certificate of incorporation and bylaws) and the core investment documents; (c) major changes to stock classes, rights or issuances; and (d) increasing or decreasing the size of the company's

board. Sometimes the protective provisions will include veto rights over the company incurring a certain amount or a certain type of debt, or the creation, amendment or termination of stock option and other equity incentive plans.

These are some of the common protective provisions, but each deal usually has some unique or bespoke protective provisions included for deal-specific reasons. In negotiating the scope of the protective provisions, deal-specific considerations, including the size of the investment, the size of the company, the existing protective provisions, and the company's financial condition all play a role in settling on the full scope of the protective provisions.

The protective provisions and other veto rights require the company to seek the required approval to take an action, it doesn't mean the company cannot undertake the specific action in perpetuity.

This leads to the second issue, which is negotiating the consent threshold (i.e., the number of investors or what percentage of stock) required to approve the matters covered by the protective provisions. In certain cases, the lead investor will push to have a specific veto but in other situations, it may be a simple majority of the investor stock (a group of investors that together hold a majority of the shares). Not all approval thresholds need to be the same. The reality is that this is a heavily negotiated control term so it is important to think about the present financing round and how the company may be set up for future rounds.

In addition to the preferred stock protective provisions, investors may also negotiate veto rights for the director(s) designated by the holders of preferred stock. Generally speaking, as a stockholder, an investor can act in their own self-interest. On the other hand, directors (including directors appointed by investors) are bound by fiduciary duties that require the directors to act in the best interests of the company/all stockholders. So, companies sometimes view preferred director veto rights as somewhat less onerous than stockholder veto rights.

9.3.3 Information Rights

Information rights obligate the company to furnish specified reports and data to its investors on a regular basis. Information rights facilitate oversight and informed decision making and give investors enhanced visibility into the company's financial condition, operational performance, and material corporate actions. Whether they are provided to all investors or only those that invest a certain amount varies from deal to deal. Companies are usually permitted to withhold information from competitors.

Examples of information rights that investors may require from the company include the right to receive regular financial statements (annual, quarterly, monthly), annual operating budgets, and periodic capitalization tables. The scope and nature of these reporting obligations are not usually heavily negotiated, and the burden is generally manageable if a company is operating with a basic financial reporting system.

Information rights may also include inspection rights that permit investors to examine the company's books and records upon reasonable notice. Information rights are generally not permanent; they often expire when the investor's ownership falls below a specified threshold or may automatically terminate upon certain events such as an initial public offering, sale of the company or dissolution.

9.3.4 Rights of First Refusal and Co-Sale

Rights of first refusal and co-sale rights give investors a measure of protection when company common stock, often the common stock held by core founders, is being transferred. These rights help prevent unwanted third parties from acquiring shares and/or allowing founders to monetize their equity holding ahead of investors. A right of first refusal allows investors and/or the company to purchase shares that a founder or other stockholder intends to sell or transfer before those shares are offered to third parties.

Co-sale rights, also referred to as "tag-along" rights, permit investors to participate in a sale alongside the selling stockholder, allowing the investor to sell a proportional share of their own holdings if a founder or key common stockholder sells their shares. These rights help investors monetize their equity alongside the selling or transferring founder.

While there are exceptions to these sale and transfer restrictions, including those that allow for founder estate or tax planning transfers, the rights of first refusal and co-sale generally have a strong deterrent effect on any proposed sales or transfers by founders or key common stockholders.

9.3.5 Drag-Along Rights

As a general rule, drag-along provisions require company stockholders to vote all of their shares in favor of a sale of the company and participate in the sale process, subject to certain conditions being satisfied. Among those conditions is approval of the Board and approval of one or more specified groups of stockholders, almost always including the investors.

The purpose of a drag-along provision is to help ensure that the sale process is smooth, that there are no minority investors who choose to threaten litigation to block a deal, and to satisfy acquirors, who frequently require supermajority (and sometimes unanimous) stockholder approval of a deal in order to consummate a transaction. Drag-along provisions are generally not heavily negotiated (other than negotiation of the triggering conditions).

In the absence of drag-along provisions in a company's governing documents, corporate transactions could be delayed or blocked because one or more stockholders (including small investors or departed common stockholders) attempt to leverage their statutory rights to secure benefits that are disproportionate to their equity position in exchange for their approval of an exit transaction. Founder and investor interests are generally aligned on this topic; it is important to avoid minority investors derailing a Board and majority stockholder-approved exit.

Once a drag-along provision is "triggered" and the necessary approval conditions are satisfied, all stockholders subject to the drag-along rights are generally required to approve the sale of the company, sign all documents necessary to consummate the sale of the company, and refrain from exercising any dissenters' or other statutory rights.

Despite the contractual agreement of the stockholders subject to the drag-along rights, delays inevitably occur from time to time as a result of stockholders failing to timely comply with their obligations. To address this issue, there is often a mechanism to compel compliance; stockholders often grant a proxy and irrevocable power of attorney to one or more company executives or agents for the purpose of approving and effecting a sale of the company after the drag along rights have been triggered.

9.3.6 Redemption Rights

Redemption rights grant investors the ability to require the company to buy back their shares after a predetermined period of time after their investment. At the time of this report, market surveys suggest that redemption rights are relatively rare and usually only arise 5 years (or more) after an investor's initial investment. These rights are intended to allow an investor to seek liquidity for their investment by forcing the company to buy back their shares.

However, this buyback right may be difficult for a company to manage if there are other competing uses of available cash. Redemption rights also often jeopardize a company's ability to issue Qualified Small Business Stock.

Further, redemption rights are generally subject to restrictions tied to the company's available cash or legal ability to make such payments under applicable law (e.g., the company is not required to fund a repurchase or redemption if it would trigger insolvency).

The terms of redemption rights typically specify the timing, process, and price for repurchasing shares, which is often based on the original purchase price, but the price term can be heavily negotiated in certain unique instances. If the company is unable to honor immediate redemption requests, additional investor protections or remedies may be triggered (such as payment of the price over time, subject to accruing interest on the unpaid amount).

9.3.7 Anti-Dilution Protection

Anti-dilution rights are a standard investor protection that is negotiated as part of an equity financing transaction. An anti-dilution provision is a mechanism that serves to adjust the economics of an investment transaction and the dilutive effect of a subsequent down-round financing (i.e., where the effective share price in a subsequent financing is lower than the per share price in a prior financing), among other transactions. Companies with valuations towards the higher end of the "market" range need to pay close attention to anti-dilution rights and preferences.

Anti-dilution protections are generally found, in the case of a corporation, in the company's certificate of incorporation and like other investor rights, they can be waived (and adjustments foregone) with the consent of the requisite rightsholders. For founders, understanding anti-dilution protection is important because it can significantly affect the distribution of equity, including common stock dilution, in the company after future fundraising rounds.

The two most common forms of anti-dilution protection are "weighted average" anti-dilution and "full ratchet" anti-dilution. Both are formula-driven adjustments. "Weighted average" anti-dilution, whether the "broad-based" or "narrow-based" weighted average method, is in almost every deal and it serves to average down the prior, higher per share price from the prior financing that closed at the higher valuation to account for the new financing at the lower valuation. The adjustment is affected via a change to the effective preferred stock-for-common stock conversion ratio. "Full-ratchet" anti-dilution is extremely rare (given its punitive economic effects). The details and effects of anti-dilution protection should be discussed with your attorney before any financing documents are finalized.

9.3.8 Pre-Emptive Rights

Pre-emptive rights, also known as "pro rata rights" or "participation rights", grant an existing investor the ability to purchase a proportionate share of any new securities (whether shares of stock or other convertible securities) that the company proposes to issue in a new financing, usually on the same terms they are offered to the new investors in the offering. One of the core purposes of preemptive rights is to allow an investor to defend their investment—if new securities are issued, they should be allowed to invest further. Further investment allows an investor to maintain the investor's percentage ownership in the company and avoid the downside risk of not having invested in the latest or most senior security.

Participation rights for SAFE holders can be in the form of the YCombinator published pro rata rights letter. For equity financing, the NVCA documents include standard participation rights terms in the model Investors' Rights Agreement.

Founders should pay close attention to the scope and nuanced terms of pre-emptive rights because they sit at the intersection of control, valuation and long-term exit strategy. A founder who fails to negotiate balanced pre-emption rights provisions may find that their next financing transaction is materially more complex; pre-emptive rights can influence investor behavior and increase the administrative burden of closing the next financing because more investors are involved. A core term to pay attention to is who controls the right to "waive" or "amend" participation rights (and how any waiver of rights may affect some or all of the participation rights holders.) Another core term is how much of a next financing the pro rata rights holders can take up (or purchase), which will impact a new lead investor's desire or ability to invest.

Careful drafting of pre-emptive rights involves negotiation of an appropriate preemptive rights notice period, limits on what the rights cover (so the company can issue certain securities without triggering the rights) and, potentially, the ability to offer investment to participation rights holders after an initial closing of the sale of new securities.

Pre-emptive rights are not a boiler-plate afterthought; they are a fundamental component of the company's long-term governance architecture and a common safeguard for investors seeking to protect both their economic and strategic interests as the startup company scales.

9.4 ECONOMIC TERMS FOR INVESTMENTS

As important, or in some cases more important, than governance and control rights are the economic terms and associated rights and privileges of the securities that a company issues to investors.

Whether it is the interest rate and valuation cap of convertible notes or the valuation, dividend rights and liquidation preference (among other terms) of preferred shares issued in an equity financing, these terms have a material impact on the company's capitalization structure and waterfall in a sale or liquidation.

Economic terms, even more so than governance and control terms, are heavily negotiated between the founding team and the investors. Assistance of advisors and experienced lawyers can help but market norms around valuation are difficult to pin down given that valuation is highly fact-specific. On the other hand, the security's liquidation preference, dividend terms and anti-dilution rights (if applicable) are substantially driven by market norms and there are studies published about what's "standard" in a financing of the type and size the company is seeking.

As with governance and control rights, there is more complexity in economic terms when a company is raising funds in an equity financing because the company is setting a formal "valuation" by selling a certain percentage of its stock for a certain amount of money. There are less variables in a convertible note or SAFE financing because the company is not directly setting a valuation on the company.

9.4.1 Valuation and Price Per Share

The pre-money valuation is a critical economic term that establishes the company's valuation as of immediately before the new cash investment and helps determine the price per share for the financing round. Valuation and the price per share tie directly to the dilution that current stockholders will experience in a financing round as the newly issued shares in the round will "dilute" current stockholders. Because the price per share, the amount of money raised, and the effective pre-money valuation allow the company to calculate what percentage of the company's equity the company is selling (and how many new shares it is issuing), this valuation term is critical. The amount of money raised is often driven by how much money the company needs to expand over the next 12-24 months and the price per share is simply a result of a formula—so the major negotiated variable is where to set the company's effective pre-money valuation.

Valuation is market-driven but the figure is the result of negotiation between founders and investors. It often reflects the company's current traction, market opportunity, and comparable transactions for companies of that size and industry. Occasionally investors will back into the company's valuation because they require a certain round size or ownership percentage post-financing.

With a higher valuation, the company will be able to sell shares at a higher price and, consequently, issue less shares than it otherwise would for a round of that size. Higher valuation and lower price per share means a smaller stake for investors in the round and less resulting "dilution" (i.e., a smaller decrease in current stockholder ownership percentages).

Careful consideration of valuation is essential, as it sets the benchmark for future rounds and influences the company's ability to attract additional capital. If the valuation is too high or too low, there is a higher risk of a later down round or unnecessary dilution. Additionally, "valuation" has many inputs so looking only at the "pre-money valuation" in a term sheet (without considering what inputs go into the price per share formula) is unwise. It is important to consider how the price per share is calculated and what inputs are included in the pre-money valuation (e.g., is an investor requiring a large increase in the option pool or are they converting convertible securities into the effective pre-money?).

Creating an accurate pro forma capitalization table or using valuation models, like Carta's pro forma capitalization table modeling tool, can be very helpful.

9.4.2 Valuation Caps, Discounts and Interest Rates

Valuation caps and conversion discounts are concepts that apply to SAFEs and convertible notes. Only convertible notes have interest rates. An equity financing may be impacted by these terms (as the equity financing will usually result in conversion of any outstanding convertible securities) but the issuance of preferred stock does not require a founder to make decisions about these three terms.

These terms also impact the conversion of securities in a sale or in another negotiated event (like conversion into stock at the maturity of a convertible note.)

A "valuation cap" is a pre-determined maximum price that an investor's convertible security (SAFE or convertible note) will convert into preferred stock at in the future equity financing. If investors invest in a convertible security, that does not directly result in the valuation of that company. But if a company uses the funds from the investment and grows materially, the investor generally will use a valuation cap as protection that the effective price they pay in the financing (the conversion price) isn't unreasonably high. Founders should review this term more fully and make sure to understand the scope and nuances of the valuation cap and whether the valuation cap is a "pre-money" cap (like a convertible note) or a "post-money" cap (like most SAFEs).

A discount functions as a similar investor protection. The discount term permits an investor to convert their investment amount into their convertible security into shares of the company's preferred stock at a discount to the valuation paid by new cash investors (e.g., if a new cash investor pays $10 for one share of Series A preferred stock and the discount is 20%, the convertible security would convert at an effective valuation of $8 per Series A preferred share).

Convertible notes, as debt instruments, will bear interest. This interest will accrue at a specified rate over the term that the convertible note is outstanding. Generally, interest that accrues is not paid to the investor and instead it would result in a larger investment balance being converted into equity at the time the note converts in an equity financing.

Discounts and valuation caps are often paired together and the effect that it can have on a company's projected cap table should be closely modeled before the company's issues and sells convertible securities to avoid a situation where there is unexpected and unnecessary dilution. Founders should also evaluate whether a convertible security will convert into a "shadow series" of preferred stock in a conversion event.

9.4.3 Liquidation Preference

Each share of a company's stock has a "liquidation preference," which refers to its position in a company's capital stack and ties to the priority for payout in an exit transaction (usually, a merger/acquisition) or a sale of the company's assets in a liquidation. Shares of preferred stock held by investors are almost always paid before (and have a higher "preference" priority than) shares of common stock.

This means that, as a general rule, holders of preferred stock are receiving their "liquidation preference" after the company has satisfied its debt obligations, but before amounts are distributed to common stockholders. Once the liquidation preferences of the preferred stock have been satisfied, the balance of any proceeds or remaining assets are typically distributed to the holders of common stock (though sometimes preferred stock will also "participate" by sharing in what remains after the initial preference is paid.) Put another way, the preferred stockholder's liquidation preferences generally dictate the manner and number of distributions to stockholders of the company in connection with a liquidity event such as a merger, sale, or liquidation of the company.

Liquidation preferences are always detailed in an equity financing term sheet because they are a core economic term. And while liquidation preferences can have a variety of different styles, there are two main components. The first is the "multiple"—whether an investor gets one times (1x) the invested capital back, two times (2x) or more. The market norm is currently a "1x" multiple. The second component is whether the preferred stock "participates" in what's left over for the common stockholders after the preferred liquidation preference(s) have been paid. Market norms currently state that "participating preferred" stock is rare and very investor-friendly.

Preferred stock sold in most early-stage equity financing rounds typically carries a "1x non-participating" preference. This means that each preferred stockholder is entitled to receive the greater of (a) one times the stockholder's invested capital (plus any accrued but unpaid dividends) and (b) the amount that would be payable to the preferred stockholder if the preferred stock were converted to common stock. The latter point is a very important nuance—in an upside event (e.g., the company's valuation increases substantially and an exit is at a multiple of the investment valuation), the investor would not be happy with their 1x and instead they can convert their preferred stock to common stock and effectively take a percentage of the sale proceeds that equals the percentage of the company they own. Following payment of the liquidation preference, the common stockholders split the balance of the proceeds or remaining assets available for distribution.

Key Considerations: Start-ups Seeking Venture Capital

- **Develop a clear value proposition.** A compelling value proposition explains precisely how the quantum solution creates measurable value beyond classical approaches. Effective narratives can help identify high-pain problems, quantify performance or cost advantages, and map those advantages to buyer priorities. Attempt to avoid vague promises of "quantum advantage" and instead specify metrics such as fidelity, throughput, latency, energy use, or time-to-solution, tied to real use cases in materials discovery, optimization, sensing, or secure communications. State clearly what you can enable today and what later generations will enable, so investors can assess timing and risk.

- **Build a strong, multidisciplinary team.** Quantum ventures should be more successful when scientific excellence pairs with engineering rigor and commercial acumen. Teams that integrate quantum physicists, control and systems engineers, software specialists, product managers, and go-to-market leaders may translate lab breakthroughs into reliable products. Advisors with domain depth in targeted verticals, such as pharma, logistics, finance, and aerospace, may strengthen credibility. Demonstrate execution through hiring, shipping prototypes, and landing pilots, which can matter more than pedigree.

- **Demonstrate technical feasibility and roadmap.** Evidence of feasibility reduces perceived risk. Credible signals may include peer-reviewed results, benchmark comparisons, functional prototypes, calibration data, error budgets, and reliability metrics. A staged roadmap may define architecture choices, anticipated performance gains, and gating milestones such as qubit count and quality, error correction thresholds, system integration, and software maturity. Identify dependencies, including but not limited to supply chains for cryogenics or photonics, control electronics, and fabrication yields, and pair each with mitigation plans and timelines.

- **Understand the market and competitive landscape.** Sophisticated market understanding goes beyond total addressable market slides. Analyze initial beachheads, quantify willingness to pay, and identify adoption triggers and procurement processes. Competitive mapping may include classical incumbents, quantum peers across modalities, and substitute solutions. Also, companies may tie clear differentiation in cost or performance, integration ease, ecosystem position, or defensible IP to a go-to-market motion that matches buyer behavior in conservative, regulated, or technically demanding sectors.

- **Protect intellectual property.** Robust IP may form barriers to entry and underpin valuation. Pursue an intentional strategy that prioritizes filings on core inventions, process know-how, control stacks, and application-specific innovations, while balancing secrecy and publication to attract talent. Freedom-to-operate analyses, jurisdictional choices, and continuation practices could also be impactful. When using standards or open-source elements, companies should document license compliance and possibly define defensible proprietary layers.

- **Prepare a scalable business model.** Scalability may hinge on repeatable production, serviceability, and unit economics that improve with scale. Hardware ventures can address manufacturing pathways, supply security,

reliability, and field support models. Software and algorithm ventures can quantify data, compute, and integration costs and show how they capture value through subscriptions, usage-based pricing, or outcome-linked models. Choosing to utilize platform approaches that enable partners and independent software vendors (ISVs) to compound network effects may reduce direct sales burden.

- **Engage with the quantum community and ecosystem.** Active participation in consortia, standards bodies, open-source projects, and government programs could accelerate credibility, talent access, and early customer discovery. Collaborations with national labs, universities, and industrial labs can de-risk technical challenges and expand non-dilutive funding. Forming strategic alliances with cloud providers, chip foundries, cryogenics vendors, or systems integrators may secure critical infrastructure and distribution channels.

- **Communicate regulatory and ethical considerations.** Quantum technologies could intersect with export controls, cryptography rules, dual-use concerns, and sector-specific regulations in healthcare, finance, and defense. Companies may choose to adopt a proactive posture, explain compliance strategy, define data governance, validate models, and implement safety protocols for sensing or communications deployments. Ethical framing can address security impacts, post-quantum cryptography transitions, and responsible research disclosures, which may assist in aligning with enterprise and government stakeholders.

- **Show traction and early validation.** Investors favor evidence that customers care and will pay. Signals may include letters of intent, paid pilots, design partnerships, cloud marketplace listings with usage, and integration into established workflows. Validation can also come from independent benchmarks, challenge wins, or co-authored case studies with industry leaders. Reporting clear learnings from pilots and showing how those learnings reshape the product and roadmap may demonstrate capital efficiency and market fit progression.

- **Tailor the pitch to venture capitalists.** A focused pitch frames the opportunity through the lens of venture-scale outcomes, including but not limited to market timing, defensibility, path to revenue, and exit scenarios. The narrative can balance technical depth with accessible explanations for general partners, supported by appendix material for technical diligence. Metrics such as runway, burn, gross margins, sales cycle, and milestone-based use of funds may help investors underwrite risk. Companies should anticipate diligence questions on reliability, supply chain, and team hiring plans to streamline the process.

- **Plan for long-term funding needs.** Quantum commercialization may span longer horizons and higher capital expenditure than typical software ventures. Sequencing technical, commercial, and regulatory milestones against trancheable capital may help to reduce dilution and risk. Blended financing, including non-dilutive grants, corporate partnerships, project financing for deployments, and customer prepayments, can extend runway. Companies should consider transparency on future round sizes, valuation logic, and scenarios for success or pivot to build investor confidence.

- **Maintain transparency and realistic expectations.** Credibility grows when you state challenges, risks, and timelines plainly. Discussing error sources, yielding limitations, integration hurdles, and market adoption barriers openly may enable collaborative problem-solving with investors and partners. Companies should set specific, measurable, and time-bound milestones, and include contingency plans for delays as well as to pair conservative claims with consistent delivery to outperform aggressive promises that slip, especially in a field with common hype cycles.

Key Considerations: Venture Capital Firms Investing in the Quantum Industry

- **Deep technical diligence.** Venture capital firms investing in quantum technology should conduct rigorous technical due diligence by engaging domain experts to assess the feasibility, scalability, and novelty of the underlying quantum science. For example, before investing in a quantum computing startup, a VC may consult with quantum physicists to evaluate the company's approach to error correction or qubit stability.
- **Long-term investment horizon.** Quantum technologies may require extended development timelines before commercialization. Successful VCs in this space could adopt a patient capital approach, understanding that returns may require a decade or more. For instance, early investors in companies like Rigetti Computing or PsiQuantum could commit to multi-year funding rounds and recognize the long path to market readiness.
- **Portfolio diversification across quantum verticals.** Given the uncertainty and breadth of quantum applications, VCs can choose to diversify investments across quantum verticals such as quantum computing hardware, quantum software, quantum communications, and quantum sensing. For example, a fund may invest in both a quantum encryption startup and a quantum materials company to hedge against technical and market risks.
- **Strategic partnerships and ecosystem building.** Venture capitalists in the quantum sector can facilitate partnerships between startups and established industry players, research institutions, or government agencies. For example, a VC may assist a quantum startup secure a collaboration with a national laboratory or a major cloud provider to accelerate development and adoption.
- **Focus on intellectual property (IP) and talent.** Strong IP portfolios and access to top-tier scientific talent may differentiate companies in quantum. VCs can choose to prioritize companies with robust patent strategies and with teams led by recognized quantum scientists. For instance, investors could direct capital to startups spun out of leading academic institutions with exclusive IP rights.
- **Active involvement in policy and standards development.** Given the nascent stage of the quantum industry, VCs can engage in policy discussions and standards-setting bodies to help shape the regulatory environment. Leading quantum investors may choose to participate in organizations like the Quantum Economic Development Consortium (QED-C) to influence policy and standards.
- **Emphasis on commercialization pathways.** Investors typically seek startups with clear, realistic go-to-market strategies and early use cases, even if full-scale quantum advantage lies years away. For example, a quantum software company could initially target hybrid quantum-classical algorithms for near-term applications in optimization or machine learning.
- **Risk mitigation through syndication.** Due to the high technical and market risks, VCs may choose to syndicate quantum deals with other investors and may also share both the risk and the expertise. For example, multiple venture funds, including New Enterprise Associates (NEA) and GV (formerly Google Ventures), jointly invested in IonQ.
- **Continuous monitoring of scientific and market trends.** The quantum landscape evolves rapidly, with frequent breakthroughs and shifting competitive dynamics. Leading VCs may choose to maintain close contact with the scientific community and update their investment theses based on the latest research and market signals.
- **Support for government and grant funding leverage.** Quantum startups often rely on non-dilutive funding from government grants and contracts. VCs can encourage portfolio companies to pursue such opportunities, which extend runway and validate technology. For example, many quantum startups in the U.S. and Europe may have chosen secured funding from agencies like DARPA or the European Quantum Flagship.

10 | Managing Financial Risk

WHY THIS MATTERS FOR THE QUANTUM SECTOR

Like other emerging technology enterprises, quantum companies face new challenges and a higher level of financial risk than businesses in more established industries. As a result, industry participants may face financial challenges in their own businesses or with counterparties more frequently than participants in mature sectors.

Investors manage financial risk in quantum investments by using a blended capital strategy, compliance-by-design, disciplined IP and data-rights planning, supply chain and cybersecurity rigor, and transaction structures that anticipate regulatory review. Together, these tools convert scientific promise into durable, investable businesses and safeguard U.S. technological leadership.

Key takeaways:

- **These financial issues can create both obstacles and opportunities for quantum companies.**
- **By understanding and anticipating these issues, and by engaging experienced legal and financial advisors, a quantum company can improve its odds of successfully navigating its financial challenges and reorganizing, rather than being forced to liquidate or sell key assets at an inopportune time.**

10.1 MANAGING FINANCIAL RISK

10.1.1 Capital Requirements and Risk in the Quantum Sector

Significant public and private capital are essential to mature the quantum sector, which demands sustained investment in basic research, specialized infrastructure, and a highly skilled workforce. Public funding, including direct appropriations, tax incentives, and competitive grants, de-risks early-stage research and innovation that may lack immediate commercial appeal while expanding the base of foundational knowledge. Private investment converts laboratory advances into products, scales manufacturing, and integrates quantum capabilities into existing supply chains. Together these funding streams create a reinforcing cycle in which public dollars validate scientific feasibility and private dollars facilitate large-scale production and commercialization, strengthening national competitiveness in a strategically important domain.

Investors may face long development timelines and elevated technical and financial risk. Quantum hardware faces persistent engineering hurdles, including qubit coherence, error correction, and cryogenic control, that may take a decade or more to resolve while generating limited near-term revenue and requiring ongoing capital. Because end markets remain nascent, even superior technologies may not gain traction before investors exhaust their risk tolerance. Cyclical liquidity constraints can compound these pressures, contributing to valuation volatility, distressed restructurings, or bankruptcies that shift uncertainty to creditors and employees.

These may create entry points for well-informed investors and strategic acquirers. Companies with credible technology but insufficient capital may accept new financing on terms that reflect the risk. Investors can also pursue opportunities in bankruptcy by purchasing businesses or strategic assets, or by providing financing that helps a company operate in reorganization and eventually exit those proceedings.

10.1.2 Investment Approach and Policy Levers

Investors may choose to deploy capital prudently in quantum by conducting rigorous technical and commercial diligence, building a diversification strategy, and maintaining extended payoff horizons consistent with venture risk. Policy makers can mitigate downside risk while preserving private incentives to innovate by using targeted tools such as milestone-based grants, matched funding, and loan guarantees. Stakeholders can aim to proceed with clear eyes. Commercialization remains uncertain, and investors can lose their entire investment, even as successful outcomes could deliver outsized returns and broad societal benefit. Given this risk profile, investors and other major participants can seek education to understand the basics of bankruptcy and related insolvency regimes.

10.2 KEY U.S. BANKRUPTCY AND SIMILAR LAWS

In the high-stakes world of quantum technology, even the most promising companies can face financial setbacks or unexpected challenges. Anyone involved in the quantum industry may educate themselves to understand U.S. federal and state laws that govern bankruptcy proceedings and other financial restructurings, because those laws may also determine the outcome when a company encounters financial distress that requires it to use a collective process to resolve its debts, such as a bankruptcy case or similar proceeding.

A company may not necessarily be going out of business the moment a company begins a bankruptcy proceeding or other financial restructuring. Some proceedings may liquidate or wind down the business, but bankruptcy and other restructurings are legal processes that can preserve a business, protect valuable assets like IP, and provide a fair way to resolve debts with creditors collectively, while helping avoid the erosion and eventual division of value through piecemeal litigation.

> In 2024, Zapata AI, a quantum software startup, filed for bankruptcy protection after it faced significant financial challenges. Instead of liquidating immediately, Zapata used the bankruptcy process to negotiate with creditors, reorganize its obligations, and develop a plan to pay down or settle its debts over time. The restructuring enabled the company to seek new investment, preserve its core technology, and continue operations. The approach showed that companies in the quantum industry can use bankruptcy as a tool to reorganize and potentially recover rather than simply shut down.

Bankruptcy laws define the types of proceedings and restructurings available to businesses and individuals, explain how parties can choose to handle debts and assets, and establish protections and obligations for both debtors and creditors. Quantum companies and their stakeholders must understand these proceedings because they offer potential options to navigate financial distress, protect valuable technology, and support informed decisions that safeguard their interests if financial trouble arises.

10.2.1 Federal Bankruptcy Law: The Bankruptcy Code (Title 11 of the U.S. Code)

Bankruptcy proceedings in the United States collectively resolve debts by aggregating a bankrupt party's (the "debtor's") assets and distributing those assets to creditors and other stakeholders in accordance with the priorities laid out in the Bankruptcy Code. The Bankruptcy Code governs all bankruptcy cases in the United States. It establishes rules and procedures for seeking relief from debts, handling assets, and paying creditors. The Bankruptcy Code contains different chapters tailored to specific situations. Several chapters relevant to quantum industry bankruptcies appear below.

- **Chapter 7: (Liquidation).** Chapter 7 proceedings liquidate the debtor. A company in Chapter 7 ceases operations and sells its business or non-exempt assets to pay creditors. A third-party trustee appointed by the U.S. Bankruptcy Court displaces the company's management and takes control of the liquidation.

For quantum companies, this may mean the sale of intellectual property, equipment, or other assets to unaffiliated purchasers for the best price available. The company does not receive a discharge debt in Chapter 7, because liquidation eliminates the company. The proceeds from the sale of the company's assets pay creditors and other stakeholders in accordance with the U.S. Bankruptcy Code.

Creditors of quantum companies may face unique challenges in a Chapter 7 proceeding. The trustee may bring actions to recover so-called preference payments that a bankrupt company made to a creditor within 90 days before the bankruptcy if those payments allowed the creditor to receive more than it otherwise would have and other technical requirements are met. A trustee may also seek to avoid and recover any transfers of money or property to creditors over multiple years before the bankruptcy if the debtor remained insolvent at the time of the transfer and did not receive reasonably equivalent value. Creditors can anticipate such claims and prepare to defend them if they arise.

- **Chapter 11: (Reorganization).** Chapter 11 primarily applies to businesses that continue operating under existing management while they restructure their debts. A company in a Chapter 11 proceeding may seek to sell its business as a going concern to a purchaser that will continue the business, reorganize its finances pursuant to a Chapter 11 plan of reorganization, or pursue other alternatives. Quantum companies in Chapter 11 proceedings have a wide range of options to restructure their business operations, including the rejection of burdensome contracts and leases.

  Chapter 11 proceedings provide debtors with tools to restructure their business's finances and operations under Bankruptcy Court supervision. Unlike in a Chapter 7 proceeding, existing management can remain in control of the debtor's business during the case. That management has the exclusive right to propose a Chapter 11 plan for the debtor for up to two years, which may give the debtor a significant period to negotiate with creditors and attempt to develop a consensual Chapter 11 plan, resolve substantial litigation, or address other impediments to making distributions to its creditors.

- **Chapter 15: (Cross-border insolvency).** Chapter 15 proceedings address U.S. recognition of foreign bankruptcy proceedings. While these proceedings occur much less frequently than Chapter 7 or Chapter 11 cases, they can present an option for quantum companies with international operations, as such proceedings help coordinate legal actions and protect assets across borders.

- **The automatic stay.** When a bankruptcy case begins, an "automatic stay" immediately takes effect. This legal protection stops most collection actions, lawsuits, and foreclosures against the debtor with respect to pre-bankruptcy debts. It gives the company or individual time to reorganize or liquidate assets without creditor pressure.

- **Trustee and creditor committees.** In Chapter 7 cases (and occasionally in Chapter 11 cases), a trustee oversees the debtor's business and affairs, manages and liquidates assets, and distributes the proceeds of asset sales to creditors in accordance with the Bankruptcy Code's priority scheme. In Chapter 11, an official committee of unsecured creditors may form to represent the interests of those creditors in the bankruptcy process. A creditors' committee participates in virtually all aspects of a bankruptcy case, hires professional advisers, and may object to actions the debtor seeks to take.

10.2.2 State Law Alternatives to Bankruptcy Proceedings

In addition to the protections afforded under federal law embodied in the Bankruptcy Code, a business can address its liabilities under state law in several ways. One option may include an assignment for the benefit of creditors (an "ABC"), in which the company transfers its assets to an assignee to liquidate the assets and distribute the proceeds to creditors. Alternatively, a company may also agree that a secured creditor (sometimes a lender) will conduct a consensual foreclosure of the business and its assets, after which the creditor can sell the assets and apply the proceeds to reduce the company's secured debt. A company can also wind down the business and then dissolve under state law; however, in that scenario the company covers all of its debts, which may not be feasible if its assets are worth substantially less than its liabilities.

State law alternatives to bankruptcy proceedings vary significantly by jurisdiction. It is important to identify which state's law governs the proceeding and how that law differs from bankruptcy proceedings governed by federal law.

10.3 CHALLENGES OF U.S. BANKRUPTCY LAWS IN THE QUANTUM INDUSTRY

10.3.1 Valuing Quantum Intellectual Property

Quantum companies may hold most of their value in patents, trade secrets, or proprietary technology. Accurately valuing those assets during bankruptcy is difficult because technology remains cutting-edge, markets continue to develop, and few comparable sales exist. These factors make it hard to determine the fair market value of quantum-related IP. This difficulty, in turn, complicates many other aspects of bankruptcy or restructuring, including whether quantum IP has sufficient value to secure loans, the appropriate price in a bankruptcy sale, and related matters.

10.3.2 Protecting Sensitive Technology

Bankruptcy proceedings are public, and selling or transferring assets can risk exposing confidential information or trade secrets. U.S. bankruptcy courts routinely consider confidential information and may approve sealing the record to protect proprietary or other sensitive materials, but parties commencing a bankruptcy case cannot assume at the outset that the court will grant protections to the degree they desire.

Competitors or foreign entities may obtain valuable quantum technology if parties do not implement safeguards to protect those assets. This risk is particularly acute in Chapter 11 cases where the debtor seeks to preserve its business while restructuring its financial affairs. Competitors or other strategic purchasers may intervene in a Chapter 11 case with superior offers to creditors and other key stakeholders that conflict with the debtor's management's objectives. A debtor can manage this risk by negotiating with key stakeholders before commencing a Chapter 11 case to align on restructuring goals, but competitors and others may also attempt to negotiate with those stakeholders to advance their own objectives regarding the debtor.

10.3.3 Navigating Complex Contracts and Licensing

Quantum companies may operate under complicated licensing agreements, research partnerships, and government contracts. The U.S. Bankruptcy Code grants a debtor the right to assume or reject executory contracts, meaning contracts with material unperformed obligations on both sides. In some cases, a debtor may also assume and assign executory contracts to a third party, such as an asset purchaser, notwithstanding anti-assignment provisions in the contract. These tools allow debtors reorganizing under Chapter 11 to shed burdensome contracts, maximize the value of their contractual relationships, and advance the U.S. Bankruptcy Code's goal of providing a fresh start after reorganization.

A debtor's power to assume, assign, or reject contracts is limited. Absent the counterparty's consent to modifications, a debtor generally can assume or reject a contract in its entirety. Additionally, bankruptcy courts may enforce certain limitations on assignment, for example when the identity of the counterparty is material to performance, notwithstanding the general rule in the U.S. Bankruptcy Code that overrides such provisions.

U.S. bankruptcy law also imposes specific rules on IP licenses. If an IP licensor, excluding trademarks, files for bankruptcy, the licensee may elect to treat the license as terminated or to retain its rights under the license, provided the licensee continues to make royalty payments. In a licensee's bankruptcy, a licensor may choose to monitor any attempts by the licensee to assign the license, as bankruptcy courts may enforce a bar on assignment depending on the circumstances.

Many contracts and IP licenses contain clauses that permit termination upon a counterparty's bankruptcy, commonly referred to as "ipso facto clauses." These clauses may be generally unenforceable in bankruptcy. However, U.S. bankruptcy law makes an exception for contracts in which applicable non-bankruptcy law prohibits assumption or assignment. Careful analysis of these issues is critical in any quantum company bankruptcy.

10.3.4 Dealing with Government Funding and Restrictions

Many quantum companies receive federal grants or work under government contracts. Bankruptcy can trigger special rules or restrictions, including requirements to return grant money, comply with export controls, or obtain government approval before transferring certain assets. Failure to follow these rules can lead to legal exposure or loss of valuable opportunities.

10.3.5 Cross-Border Issues

Quantum businesses may choose to have international investors, operations, or IP. Coordinating bankruptcy proceedings across multiple legal systems is complex and can delay asset sales or debt resolution. Foreign jurisdictions may decline to recognize or give effect to U.S. bankruptcy court rulings, and foreign creditors may take action against a bankrupt company's assets located outside the United States. Protecting such assets could require commencing court proceedings in foreign jurisdictions to obtain recognition of a U.S. bankruptcy proceeding or commencing a Chapter 15 case in the United States to obtain recognition of foreign proceedings.

10.3.6 Maintaining Operations During Uncertainty

Bankruptcy can create uncertainty for employees, customers, and partners. Key staff may depart, customers may hesitate to sign new deals, and partners may doubt the company's future. Many customers and vendors, particularly those located outside the United States, may also believe that commencing bankruptcy necessarily means a company will go out of business, and they may reduce or terminate their relationships with the company as a result. A lengthy restructuring process can also hinder recruiting new talent needed for post-bankruptcy growth. These dynamics can make it harder to keep the business running or to reorganize successfully.

10.3.7 High Costs and Time Demands

Bankruptcy requires legal counsel, financial experts, and court oversight. In Chapter 11 cases, a company may also need to obtain new financing and pay the fees and expenses of certain creditors involved in the case, such as an official creditors' committee. For quantum companies, the need for specialized knowledge, particularly to value and protect technology, can make the process more expensive and time consuming.

These challenges may require quantum companies facing bankruptcy to plan carefully, seek knowledge-based advice, and take extra steps to protect their technology and relationships. Quantum companies choose to engage advisors early so they can understand the business thoroughly, develop restructuring solutions with management, and implement those solutions without undue time pressures or artificial constraints. Understanding the unique risks and requirements of bankruptcy in the quantum industry and preparing carefully for all eventualities can help companies and stakeholders make better decisions and preserve as much value as possible.

Key Considerations: Navigating Bankruptcy Options

- **Seek expert legal and financial advice early.** Bankruptcy law is complex, and the quantum industry adds extra layers of difficulty due to its technical nature and valuable IP. Quantum companies entering a bankruptcy proceeding should work with lawyers and financial advisors who have experience in both bankruptcy and technology sectors. By addressing problems in their early stages, a company can maximize flexibility to solve financial issues, avoid costly mistakes, and protect key assets. Creditors and other stakeholders in quantum companies may also seek early advice so they can identify signs of financial distress or operational problems in their counterparties, address issues, and pursue opportunities that might include acquiring the distressed business or key assets, providing financing, and taking other actions before the counterparty's financial issues escalate.

- **Consider all options before a bankruptcy filing.** A bankruptcy proceeding is one of the most consequential steps a company can take. Directors and officers should thoroughly inform themselves about all financial and operational restructuring options before authorizing a bankruptcy filing. In some cases, these options may allow the company to avoid bankruptcy altogether or enter a bankruptcy case in a stronger position.

- **Carefully prepare the bankruptcy filing.** Companies are advised to work with legal and finance advisers to organize their finances and affairs before filing to help facilitate a smooth transition into the bankruptcy process and minimize operational disruption. Preparing a thoughtful public relations and outreach plan can reassure customers, vendors, employees, investors, and other critical stakeholders that the business intends to continue operations and emerge from its reorganization or sale process with improved operations and a stronger capital structure. Defining the intended outcome of the bankruptcy process could help all parties work toward that goal during preparation and throughout the case.

- **Review and organize contracts and licenses.** Before filing, companies should review all contracts, licenses, and partnership agreements and try to identify bankruptcy clauses to understand their effect and evaluate whether a court will likely enforce them. Companies can decide whether to assume agreements, assume and assign them to a third party, or reject them. Organize documentation so you can respond quickly to questions from the court, creditors, potential buyers, and other key stakeholders, and can try to minimize the costs and time associated with the proceeding. Debtors may need to file much of this information with the Bankruptcy Court and provide it to creditors and other stakeholders. Gathering and maintaining this information in an organized manner before filing will help avoid unnecessary delays during the proceeding and minimize costs.

- **Communicate clearly with stakeholders.** Bankruptcy creates uncertainty for employees, investors, customers, and partners. This uncertainty can be alleviated by communicating plans and the process transparently, proactively, and accurately. Clear communication maintains trust, can help with retention of key staff, and keeps operations as stable as possible during a difficult time.

- **Plan for government funding and compliance.** A debtor in bankruptcy that has received government grants or works on government contracts should identify the special rules that apply in such circumstances. The debtor may need to notify government agencies, return unused funds, or obtain approval before transferring certain assets. Failure to follow these rules risks legal consequences and the loss of future opportunities

- **Prepare for cross-border issues.** Companies with international operations or investors can coordinate with legal experts in other countries to manage assets and legal proceedings across borders. This coordination helps avoid delays and ensures compliance with all relevant laws. Foreign laws can be reviewed to ensure the commencement of a U.S. bankruptcy proceeding does not create unintended consequences for foreign affiliates, including cross-defaults under financing documents or material contracts. Companies may need to take proactive steps in foreign countries to secure assets from potential claims by foreign creditors, and obtain foreign recognition of a U.S. bankruptcy proceeding, or recognition of a foreign proceeding in the United States under Chapter 15 of the Bankruptcy Code if necessary to protect the enterprise's assets and business wherever they are located.

- **Key consideration points for creditors and other stakeholders.** Companies should carefully monitor major suppliers, customers, and contract counterparties for signs of financial distress, including public statements, debt refinancings, delayed payments, or an increase in payment or collections-related lawsuits. Companies may also choose to enforce regular payment terms and conditions. Consider alternative sourcing to minimize exposure to a distressed supplier.

- **Look for opportunities.** Although bankruptcy presents many challenges, it also creates substantial opportunities. A distressed party's situation may allow a buyer to enter or expand in a field or business line with an established operation at a relatively low cost. Another party's bankruptcy may also present opportunities to obtain key assets, technology, or contracts. Identifying potential opportunities and carefully engaging experienced legal and financial advisors to execute on them, you can turn a distressed situation into an opportunity for non-bankrupt parties to advance their businesses quickly and at lower-than-expected costs.

Visit https://chicagoquantum.org/quantum-law-navigator and subscribe to receive updates on the Quantum Law Navigator project. We welcome ideas and feedback. Please reach out to the QLN team at QLN@uchicago.edu.