

Corporate Governance as National Security Strategy - Supply Chain Resilience as an Oversight Duty

Law Working Paper N° 919/2026

April 2026

Kish Parella

Washington and Lee University and ECGI

Carla Reyes

Southern Methodist University

© Kish Parella and Carla Reyes 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

This paper can be downloaded without charge from:
http://ssrn.com/abstract_id=6495958

<https://ecgi.global/content/working-papers>

ECGI Working Paper Series in Law

Corporate Governance as National Security Strategy - Supply Chain Resilience as an Oversight Duty

Working Paper N° 919/2026

April 2026

Kish Parella
Carla Reyes

Abstract

The nation's security depends on decisions made in corporate boardrooms: Corporations own, control and govern the critical physical and digital infrastructure upon which we daily depend. The strength of this infrastructure depends on the routine decisions made by the directors and officers who govern these corporations – choices relating to risk management, strategic development, sourcing, growth, and investments. The public stakes of these choices transform traditionally internal matters of corporate governance into contemporary issues of national security. But these corporate decisions are driven by market incentives, not security objectives, creating a significant problem of misalignment between corporate decision-making and national security policy. Multiple White House administrations have sought to address this misalignment through enhanced public governance using both executive orders and direct equity investments in corporations – measures that signal a potential re-calibration in the relationship between state and industry while still failing to reach the full range of corporations whose ordinary decisions determine national security outcomes. This Article argues that private governance – through corporate law – offers an alternative strategy to align incentives across a broader swath of corporations than those currently reached through executive action. The mechanism of this alignment is the Caremark doctrine that serves as the channel through which external national security risks become internal corporate obligations. This fiduciary duty supplies the incentive, lacking in other governance frameworks, to reconcile the public interest in infrastructure with the private interests of those who control it. It thereby offers a private law solution to public law governance gaps – one that achieves national security objectives while respecting the traditional boundary between state and industry. This Article makes three important contributions for corporate management, policymakers, and scholars. First, it identifies corporate governance as a part of national security governance, thereby reframing routine board decisions into sites of national security risk. Second, it addresses misaligned incentives between corporate governance and national security by providing a new understanding of Caremark's doctrine. Third, it offers a governance framework to guide corporate management in fulfilling their Caremark duties where national security risks are real but regulation is incomplete. It applies this framework to a case study – Bitcoin mining, an increasingly important component of U.S. digital infrastructure.

Keywords: Corporate governance; oversight duties; Caremark duties; national security; critical infrastructure; digital infrastructure; tech; cryptocurrencies

Kish Parella*

James P. Morefield Professor of Law
Washington and Lee University
483 Lewis Hall
Lexington, VA 24450, USA
e-mail: parellak@wlu.edu

Carla Reyes

Associate Professor of Law
Southern Methodist University
3315 Daniel Avenue
Dallas TX 75205, USA
e-mail: carla.reyes@smu.edu

*Corresponding Author

Corporate Governance *as* National Security Strategy

Supply Chain Resilience as an Oversight Duty

Kishanthi Parella[†] & Carla L. Reyes^{††}

ABSTRACT

The nation's security depends on decisions made in corporate boardrooms: Corporations own, control and govern the critical physical and digital infrastructure upon which we daily depend. The strength of this infrastructure depends on the routine decisions made by the directors and officers who govern these corporations – choices relating to risk management, strategic development, sourcing, growth, and investments. The public stakes of these choices transform traditionally internal matters of corporate governance into contemporary issues of national security. But these corporate decisions are driven by market incentives, not security objectives, creating a significant problem of misalignment between corporate decision-making and national security policy. Multiple White House administrations have sought to address this misalignment through enhanced public governance using both executive orders and direct equity investments in corporations – measures that signal a potential re-calibration in the relationship between state and industry while still failing to reach the full range of corporations whose ordinary decisions determine national security outcomes.

This Article argues that private governance – through corporate law – offers an alternative strategy to align incentives across a broader swath of corporations than those currently reached through executive action. The mechanism of this alignment is the *Caremark* doctrine that serves as the channel through which external national security risks become internal corporate obligations. This fiduciary duty supplies the incentive, lacking in other governance frameworks, to reconcile the public interest in infrastructure with the private interests of those who control it. It thereby offers a private law solution to public law governance gaps – one that achieves national security objectives while respecting the traditional boundary between state and industry.

This Article makes three important contributions for corporate management, policymakers, and scholars. *First*, it identifies corporate governance as a part of national security governance, thereby reframing routine board decisions into sites of national security risk. *Second*, it addresses misaligned incentives between corporate governance and national security by providing a new understanding of *Caremark*'s doctrine. *Third*, it offers a governance framework to guide corporate management in fulfilling their *Caremark* duties where national security risks are real but regulation is incomplete. It applies this framework to a case study – Bitcoin mining, an increasingly important component of U.S. digital infrastructure.

[†] James P. Morefield Professor of Law, Washington and Lee University School of Law; Research Member, European Corporate Governance Institute (ECGI).

^{††} Associate Professor, Southern Methodist University Dedman School of Law; Faculty, Initiative for Cryptocurrency and Contracts (IC3).

TABLE OF CONTENTS

INTRODUCTION	3
I. THE PUBLIC RISKS OF PRIVATE CONTROL: CRITICAL INFRASTRUCTURE AS A NATIONAL SECURITY PRIORITY	11
II. THE PROBLEM OF MISALIGNED INCENTIVES BETWEEN MARKETS AND SECURITY	14
III. ALIGNING CORPORATE INCENTIVES THROUGH PUBLIC GOVERNANCE: EXECUTIVE ACTION.....	17
A. Executive Orders on Supply Chain Resilience 2021-2025	17
B. “Executive Shareholderism”: Building Supply Chain Resilience Through Government Equity Stakes in Companies	19
C. Limitations of Executive Actions	21
IV. ALIGNING CORPORATE INCENTIVES THROUGH PRIVATE GOVERNANCE: THE <i>CAREMARK</i> APPROACH	24
A. <i>Caremark</i> Has Always Been About Critical Infrastructure	25
1. Food and Agriculture	25
2. Healthcare and Public Health	26
3. Transportation Systems	28
4. Energy	30
5. Financial Services	31
6. Commercial Facilities	32
B. Supply Chain Resilience as a <i>Caremark</i> Duty	35
V. OPERATIONALIZING <i>CAREMARK</i> : A FRAMEWORK FOR SUPPLY CHAIN OVERSIGHT	37
A. Introducing the Framework: Mapping Supply Chains, Identifying Risks, and Distinguishing Tiers	37
B. Applying the Framework: Bitcoin Mining Supply Chains as a Case Study	39
CONCLUSION	51

INTRODUCTION

When we think of national security, we often imagine traditional military assets – tanks, missiles, fighter jets, drones, and munitions. But successive White House administrations have increasingly recognized that national security extends beyond weapons systems to encompass the resilience of national critical infrastructure.¹ That infrastructure is both *physical* – power plants, highways, bridges, ports – and *digital*, including the internet. This prioritization reflects an expansive understanding of national security, one that extends beyond the defense industrial base to include the broad range of companies that provide critical infrastructure to the nation, from information technology (Google) and healthcare (Pfizer) to food and agriculture (Cargill) and energy (Chevron).

While essential to national security, critical infrastructure is largely owned, operated and governed by individual corporations. This transforms traditional matters of corporate governance – risk management, strategic development, compliance and oversight – into matters of national security because these decisions directly impact the strength or weakness of those infrastructure sectors deemed essential to the security of the nation. It also raises the stakes of corporate governance so that a failure of oversight is a national security risk.

Recent experience illustrates this dynamic: Verizon is not a part of the defense industrial base; instead, it is the largest mobile carrier in the United States. But a failure of its services can create national security risks even if it is not directly subject to national security regulation. On January 14, 2026, Verizon experienced an outage that left close to 200,000 users without the ability to use data, make calls or send text messages for several hours and up to half a day.² On January 16, Andrew R. Garbarino, Chairman of the House Committee on Homeland Security, sent a letter to Verizon’s chief executive officer requesting a briefing because of Verizon’s failure to explain the cause of the outage.³ This

¹ Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience, The White House (Feb. 12, 2013) (“It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats”) <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (accessed Jan. 23, 2026) [hereinafter PPD-21]; Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, (May 15, 2019), <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/> (accessed January 23, 2026); U.S. Nat’l Cybersecurity Strategy 1 (Mar. 1, 2023) (“Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity.”), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

² Joanna Stern, *The Day the Cell Towers Died*, WALL ST. J. (Jan. 15, 2026).

³ Letter from Andrew R. Garbarino, Chairman of the House Committee on Homeland Security, to Dan Schulman, Chief Executive Officer, Verizon Communications Inc. (Jan. 16, 2026) (“The scale and duration of the outage raises serious concerns and questions regarding the strength and security of the Verizon network. These concerns include reliability for emergency services and impact on both state and federal government operations. As of today, Verizon has

Congressional attention confirms that Verizon's disrupted service is not simply a matter of customer service but a matter of national security. This incident provides a warning about the fragility of national critical infrastructure that is provided, managed, and governed by corporate actors.

One reason for such failures is misaligned incentives between the public interest in infrastructure and the private interests of those who control it: Corporate executives respond to incentives created by the marketplace, which may not lead to optimal results under national security objectives. The U.S. National Cybersecurity Strategy found that "[t]oday's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents."⁴ Different White House administrations have sought to correct this misalignment through enhanced public governance – most recently culminating in direct equity investments in corporations, signaling a turn towards heightened federal involvement in the internal affairs of corporations deemed vital to national security. But, as providers of critical infrastructure, that category of corporations can prove expansive, thereby inviting future federal involvement in corporate affairs.

In contrast, this Article argues that corporate law offers an alternative strategy that avoids increased federal involvement while still aligning incentives between the marketplace and national security objectives. Specifically, the *Caremark* doctrine operates as the transmission mechanism through which external national security risks cross the boundary of the corporation to influence internal decisions about risk, capital allocations, and oversight. This doctrine exposes directors and officers to liability if they “utterly fail[] to implement any reporting or information system or controls” or, having done so, “consciously fail[] to monitor or oversee its operations.”⁵ Corporate law scholars have recognized that *Caremark* cases frequently involve both private harms and some form of public harm, such as loss of human life⁶ or agency action that made directors aware of compliance problems with positive law.⁷

yet to provide a sufficient public explanation regarding the cause of the outage.”), <https://homeland.house.gov/wp-content/uploads/2026/01/2026.01.16-Letter-to-Verizon.pdf> (last accessed Jan. 23, 2026).

⁴ U.S. Nat'l Cybersecurity Strategy, *supra* note 1 at 8; *id.* at 20 (“Markets impose inadequate costs on—and often reward—those entities that introduce vulnerable products or services into our digital ecosystem. Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance.”).

⁵ *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

⁶ See Robert E. Bishop & Frank Partnoy, *Corporate Oversight & Risk to Human Life* at 1 (2026)(unpublished manuscript)(“We argue that the adjudication of corporate oversight ‘Caremark’ claims should vary based on the extent to which the challenged oversight failures posed an ex ante risk to human life.”).

⁷ Tammi S. Etheridge & Carliss Chatman, *Federalizing Caremark*, 70 UCLA L. REV. 908 (2023)(“If there is a proven violation of a federal rule or regulation or other red flag provided by federal administrative agencies, the *Caremark* standard should be established, allowing shareholders to survive a motion to dismiss, shifting the burden to the directors to prove otherwise.”).

In contrast, this Article explains that *Caremark* has always been concerned with the preservation of critical infrastructure – *that* is the public harm that inadequate board oversight creates, such as risks to the healthcare sector (availability of critical drugs),⁸ transportation sector (safety of aviation),⁹ or food and agriculture sector (the health of consumers),¹⁰ among other infrastructure sectors. This is why *Caremark* demands particular attention by those who provide critical infrastructure; the consequences of their failure are too high.

The cases at the heart of the *Caremark* canon—*Caremark* and *Ritter*—involved risks to critical infrastructure caused by compliance failures. *Caremark* involved firm-level compliance failures that adversely affected the nation’s healthcare infrastructure because of the board failure to identify, prevent, or put an end to a Medicare and Medicaid kickback scheme.¹¹ *Stone v Ritter* concerned a financial institution’s failure to adequately comply with the Bank Secrecy Act’s requirements to combat money laundering,¹² thereby endangering the nation’s financial infrastructure. Subsequent *Caremark* claims have remained faithful to this origin: the cases most successfully asserting *Caremark* claims involved compliance failures related to critical infrastructure.

Using *Caremark*, this Article offers a private law solution to public law governance gaps – one that reaches a broader set of corporations than those currently subject to recent executive actions or other regulatory regimes, but who nonetheless make consequential decisions on infrastructure. By doing so, this Article reconceptualizes corporate governance as an important but unrecognized mechanism of national security policy.

This insight is critical for both public and private actors. Corporate boards – outside the defense industrial base – may fail to recognize the national security implications of their decisions. Conversely, national security policymakers may fail to account for how decisions made in corporate boardrooms affect the success or failures of their objectives. Neither corporate leaders nor political leaders need to prefer this interdependence for its consequences to materialize. Verizon’s board oversight of software issues directly endangered an infrastructure sector – communications. That is true whether its board favors a particular policy or even wants to be in the business of national security.

But corporate management cannot ensure the viability of the critical infrastructure they provide without ensuring the resilience of their supply chains. Through multiple executive orders, the executive branch has recognized the importance of supply chain resilience to the preservation of national critical

⁸ *In re Clovis Oncology, Inc. Derivative Litig.*, 2019 BL 373697 (Del. Ch. Oct. 01, 2019).

⁹ *In re The Boeing Co. Derivative Litig.*, 2021 BL 337478, at *27 (Del. Ch. Sept. 07, 2021).

¹⁰ *Marchand v. Barnhill*, 212 A.3d 805, 807 (Del. 2019).

¹¹ *In re Caremark Int’l Inc. Derivative Litig.*, 698 A.2d 959, 962-63 (Del. Ch. 1996).

¹² *Stone v. Ritter*, 911 A.2d 362 at 365.

infrastructure.¹³ In 2025, the Trump administration adopted another strategy to strengthen U.S. supply chains by taking a 10%-15% equity stake in over half a dozen companies¹⁴ deemed vital to particular infrastructure sectors.

But it is not only physical supply chains that uphold critical infrastructure. The nation's security also depends on critical *digital* infrastructure, such as the internet, email, or software without which physical infrastructure cannot operate. Disruptions to these services can also bring the nation to a halt. For example, the January 2026 Verizon service outage was caused by a software malfunction.¹⁵ A similar incident occurred on October 25, 2025 when the internet suffered a temporary outage due to a failure of digital infrastructure.¹⁶ The consequence was that internet users lost access to online services such as Snapchat, Roblox, Fortnite, Signal, Robinhood and even applications for Starbucks and McDonald's.¹⁷ The cause was an outage at the Amazon Web Services (AWS) east region datacenter.¹⁸ The outage was not due to a hardware

¹³ Exec. Order No. 14017, AMERICA'S SUPPLY CHAINS, 86 Fed. Reg. 11849 (Mar. 1, 2021); Exec. Order No. 14123, WHITE HOUSE COUNCIL ON SUPPLY CHAIN RESILIENCE, 89 Fed. Reg. 51,949 (June 21, 2024) ("Characteristics of resilient supply chains include greater domestic production; a diverse and agile supplier base; built-in redundancies; a reliable transportation system; secure critical infrastructure; adequate stockpiles; safe and secure data networks; reliable food systems; and a world-class, globally competitive American manufacturing base and workforce."); Executive Order 13806, ASSESSING AND STRENGTHENING THE MANUFACTURING AND DEFENSE INDUSTRIAL BASE AND SUPPLY CHAIN RESILIENCY OF THE UNITED STATES, 82 Fed. Reg. 34597 (July 26, 2017); Exec. Order 13817, A FEDERAL STRATEGY TO ENSURE SECURE AND RELIABLE SUPPLIES OF CRITICAL MINERALS, 82 Fed. Reg. 60835 (Dec. 26, 2017); Executive Order 13953, ADDRESSING THE THREAT TO THE DOMESTIC SUPPLY CHAIN FROM RELIANCE ON CRITICAL MINERALS FROM FOREIGN ADVERSARIES AND SUPPORTING THE DOMESTIC MINING AND PROCESSING INDUSTRIES, 85 Fed. Reg. 62539 (Oct. 5, 2020). In his second administration, President Trump issued additional executive orders to ensure U.S. pharmaceutical supply chain resilience and created a Food Supply Chain Security Task Force within the Department of Justice and the Federal Trade Commission to investigate anti-competitive behavior U.S. food supply chains. Addressing Security Risks from Price Fixing and Anti-Competitive Behavior in the Food Supply Chain, Executive Order (Dec. 6, 2025) [hereinafter Exec. Order of Dec. 6, 2025], <https://www.whitehouse.gov/presidential-actions/2025/12/addressing-security-risks-from-price-fixing-and-anti-competitive-behavior-in-the-food-supply-chain/>.

¹⁴ The Administration also take a "golden share" in U.S. Steel and has suggested that it may take an equity stake in defense contractors such as Lockheed Martin. Sarah Bauerle Danzman, *Did Trump Effectively Nationalize US Steel with his 'Golden Share'?*, ATLANTIC COUNCIL (June 16, 2025), <https://www.atlanticcouncil.org/blogs/new-atlanticist/did-trump-effectively-nationalize-us-steel-with-his-golden-share/>.

¹⁵ Caroline Anschutz, *We Finally Know What Caused the Verizon Outage, and it Wasn't What Many Assumed*, SLASHGEAR (Jan. 22, 2026), <https://www.slashgear.com/2082557/verizon-outage-cause-january-2026/>.

¹⁶ Emil Sayegh, *The AWS Outage that Shook the Internet: What it Means for Cloud Reliance*, FORBES (Oct. 20, 2025 7:34 am EDT), <https://www.forbes.com/sites/emilsayegh/2025/10/20/the-aws-outage-that-shook-the-internet-what-it-means-for-cloud-reliance/>.

¹⁷ *What to Know About the Amazon Web Services Outage*, PBS WORLD NEWS (Oct. 20, 2025 4:20 PM EST), <https://www.pbs.org/newshour/world/what-to-know-about-the-amazon-web-services-outage>.

¹⁸ Safiyah Riddle, *The Reality is Its' All Very Concentrated: AWS Outage Exposes the World's Internet Chokepoint, One Data-Center Cluster in Virginia*, FORTUNE (Oct. 21, 2025),

failure; instead, the problem was a malfunction of the control plane.¹⁹ This meant that the chain of code that provides data to operate the internet was disrupted—a break in the *data supply chain* that supports the internet. The result was an internet crash.²⁰

Data supply chains²¹ are as integral to critical digital infrastructure as roads and bridges are to critical physical infrastructure.²² A break in data supply chains can disrupt economic transactions on a wide scale, especially with the rise of emerging technologies. In January 2026, Michael Selig, Chairman of the Commodity Futures Trading Commission (CFTC), announced a “golden age” of U.S. financial markets as cryptocurrencies, artificial intelligence, and cloud computing, among other technologies, revolutionize U.S. financial markets.²³ But these technologies are only as good as the data supply chains that they run on. A break in their data supply chains can bring them down the same way that a software malfunction crippled cell phone use for over 1.5 million people and the malfunction of the control plane crashed the internet. But here, the stakes are high as these technologies are increasingly integrated into another aspect of critical infrastructure—the financial sector. A break in the data supply chains might cause widespread economic chaos if these technologies cannot perform. That is why corporate directors and officers who supply critical digital infrastructure should oversee the resilience of their data supply chains with the same care required of those who supply critical physical infrastructure. This is not an extension of the *Caremark* doctrine but a recognition of the public function it has always served, even in the shadows.

By reimagining the *Caremark* doctrine, this Article fills important gaps in multiple areas of legal scholarship. When corporate law scholars consider national security, they focus on how the latter frequently enhances compliance and regulatory requirements for corporate transactions. For example, some scholars analyze the ways that national security reviews increasingly affect both inbound

<https://fortune.com/2025/10/21/why-did-amazon-web-services-fail-virginia-data-center-outage-internet/>.

¹⁹ Sayegh, *supra* note 16.

²⁰ Juan Ortiz Freuler, *The Weaponization of Private Corporate Infrastructure: Internet Fragmentation and Coercive Diplomacy in the 21st Century*, GLOBAL MEDIA & CHINA 1, 2 (2022).

²¹ Carla L. Reyes & Kishanthi Parella, *Data Supply Chains* (January 19, 2026) (defining a “data supply chain” as “networks of transactions that transfer data as an intermediate good between individuals, organizations and technology to create a product or service for an end user”) available at SSRN: <https://ssrn.com/abstract=>.

²² U.S. Dep’t of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (2013) [NIPP 2013]; *reaffirmed* NSM-22 THE WHITE HOUSE NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Apr. 30, 2024) [NSM-22] (designating “Information Technology” as a critical infrastructure sector and defining it to include industry, assets and services that “[p]roduce[] information technology . . . include[ing] hardware manufacturers, software developers and service providers, as well as the Internet as a key resource.”).

²³ Commodity Futures Trading Comm’n, Press Statement, *Chairman Selig: America’s Financial Markets are ready for a Golden Age* (Jan. 20, 2026).

and outbound investments.²⁴ Other scholars describe Department of War efforts to reconcile the tensions between the boardroom and the war room with the explicit involvement of military personnel in corporate governance.²⁵ But these examples concern very specific situations when the national security risks are evident. They do not apply to the majority of corporate decision-making when those risks are less obvious.

Law and technology scholars have rightly focused on ways to mitigate social harms caused by this new infrastructure.²⁶ Some scholars examine the intersection between digital infrastructure and national security but focus on the impact of fragmentation²⁷ because of actions taken in the name of national security.²⁸ Other scholars examine the monopolization of digital infrastructure,²⁹ while others consider the social impact of corporate control over foundational technologies.³⁰ But few scholars have examined the impact of corporate governance on the availability of digital infrastructure.³¹

This Article fills these scholarly gaps and provides three contributions to both scholars and practitioners seeking to understand the relationship between corporate law, national security policy, and infrastructure resilience. *First*, it offers a new understanding of recent *Caremark* case law by explaining how

²⁴ Kristen E. Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549, 551 (2023).

²⁵ Andrew Verstein, *The Corporate Governance of National Security*, 95 WASH. U. L. REV. 775, 792 (2018) (describing strategies used by “Defense Security Service (DSS), a division of the Department of Defense, and are mostly applicable to military contractors with some degree of foreign ownership”).

²⁶ See, e.g., DANIELLE KEATS CITRON, *THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE* (2022); IGNACIO CALFONE, *THE PRIVACY FALLACY: HARM & POWER IN THE INFORMATION ECONOMY* (2023); JULIE E. COHEN, *BETWEEN TRUTH & POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* (2019); Amanda Parsons & Salome Viljoen, *Valuing Social Data*, 124 COLUM. L. REV. 993, 1050-53 (2024).

²⁷ See, e.g., Anupam Chandler & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015); Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT’L ECON. L. 245 (2018); ANU BRADFORD, *DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY* (2023).

²⁸ Anupam Chander, *The National Security Internet*, 114 GEO L.J. (2025).

²⁹ See, e.g., Daniel McIntosh, *We Need to Talk About Data: How Digital Monopolies Arise and Why They Have Power and Influence*, 23 J. TECH L. & POL’Y 185 (2019); Simon Lertschcher & Leslie M. Marx, *Digital Monopolies: Privacy Protection or Price Regulation?*, 71 INT’L J. INDUSTRIAL ORG. (2020); Nikolas Guggenberger, *Moderating Monopolies*, 38 BERKELEY TECH. L.J. 119 (2023); Ramsi Woodcock, *Digital Monopoly Without Regret*, 1-2020 CONCURRENCES 53 (2020).

³⁰ See, e.g., YACHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006); JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* (2009); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019).

³¹ But see Pierluigi Matera, *From Red Flags to Black Boxes: Corporate Oversight in the Age of Artificial Intelligence*, 100 ST. JOHN’S L. REV. ____ (2026), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6161886 (“The introduction of AI thus raises a familiar question in a new form: what counts as a reasonable oversight system when information is generated, filtered, and prioritized by algorithmic processes that directors neither design nor directly operate?”)

Delaware courts have denied case dismissal in situations when failed oversight created risks to national critical infrastructure. For example, Boeing's failed oversight of safety standards not only harmed the company but also reduced the fleets of national and regional airlines, thereby compromising the aviation sector's ability to transport individuals across the country.³² Similarly, Clovis Oncology's failure to oversee compliance with FDA clinical trial protocols both undermined its own approval prospects and jeopardized the prospects of a competitor's rare cancer drug to reach the market.³³ These are examples of the national costs to board dysfunction. Corporate law recognizes it; fiduciary duties correct it.

Second, this Article explains the centrality of supply chains to preserving critical infrastructure. For example, it summarizes executive action—across multiple White House administrations—that strengthen supply chains for semiconductors, rare earth minerals, and other resources to secure the critical infrastructure sectors they support. This executive focus on supply chains makes it clear that corporate directors' and officers' oversight duties extends to matters affecting the resilience of their supply chains: Supply chain resilience is an oversight duty.

Third, this Article applies these insights to critical digital infrastructure, such as the internet and email. This infrastructure is increasingly absorbed into traditional infrastructure sectors, such as financial services and transportation services. The result is that if the digital infrastructure goes down, so do the other sectors that depend on it. For example, the Verizon outage disrupted the trucking industry because modern trucking operates on cloud-based systems that rely on cell towers.³⁴ The Verizon disruption meant that truck drivers "lost visibility via electronic logging devices (ELDs), AI dashcams, GPS tracking, and driver messaging."³⁵ Society increasingly relies on digital products and services for almost every aspect of human life, thereby rendering the security of digital infrastructure a national priority. The guardians of that security are individual corporate directors and officers whose oversight of their physical and data supply chains determines the viability or vulnerability of the digital infrastructure upon which we depend.

This Article offers a framework on how corporate management should oversee supply chains that support digital infrastructure. It applies its framework to a case study of Bitcoin mining, the means by which individuals and organizations

³² Thomas Kaplan, Ian Austen, and Selam Gebrekidan, *Boeing Planes Are Grounded in U.S. After Days of Pressure*, N.Y. TIMES (Mar. 13, 2019).

³³ *In re Clovis Oncology, Inc.*, 2019 BL 373697, at *4.

³⁴ Verizon Outage Reveals Trucking's Hidden Reliance on Cell Networks, INSIDE TOWERS (Jan. 20, 2026), <https://insidetowers.com/verizon-outage-reveals-truckings-hidden-reliance-on-cell-networks/>.

³⁵ *Id.*

acquire new Bitcoins. Bitcoin is the cryptocurrency of the Bitcoin protocol,³⁶ a type of distributed ledger technology (DLT),³⁷ which allows parties to transact without even knowing each other because they use networked computers to reach agreement about the validity of records of transactions shared between them.³⁸ Bitcoin mining is increasingly important as both the federal government and individual states have declared their intent to create strategic reserves of cryptocurrencies, including bitcoin.³⁹ In November 2025, Texas bought \$5 million of bitcoin as part of its Strategic Bitcoin Reserve, making it the first state to purchase and hold bitcoin with state funds.⁴⁰ Bitcoin mining depends on two distinct supply chains: a physical (analog) supply chain and a data supply chain. This Article provides an explanation of each; identifies sources of risk to both; and provides guidance on how corporate management can ensure the resilience of the two. The creation of public strategic reserves of Bitcoin means that a failure to ensure supply chain resilience of Bitcoin mining operations can lead to significant national economic disruptions.

The Article proceeds as follows: Section I explains the importance of critical infrastructure – both physical and digital – to national security, while Section II identifies the risks created by misaligned incentives between market forces and national security objectives. It provides examples of recent national crises when different infrastructure sectors were threatened by corporate mismanagement of their supply chains. Section III explains how the executive branch has attempted to address these crises and prevent new ones by issuing a range of

³⁶ Carla L. Reyes, *Emerging Technology's Language Wars: Cryptocurrency*, 64 WM. & MARY L. REV. 1193, 1212 (2023). It is customary to use capital Bitcoin when referring to the Bitcoin protocol, and lower-case bitcoin when referring to the cryptocurrency. Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 846 n.41 (2015) (citing *Vocabulary*, BITCOIN.ORG, <https://bitcoin.org/en/vocabulary>). The authors use the capital Bitcoin mining because Bitcoin mining is an operation performed on the protocol.

³⁷ GARRICK HILEMAN & MICHEL RAUCHS, GLOBAL BLOCKCHAIN BENCHMARKING STUDY 11–12 (Cambridge Ctr. for Alt. Fin. 2017). Distributed ledgers are a type of distributed database that “assume[s] the presence of malicious users (node)” and structures data processing to attempt to thwart those malicious nodes. *Id.*

³⁸ Richard Gendal Brown, *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services* (Apr. 5, 2016), <https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/>; DANIEL T. STABILE, KIMBERLY A. PRIOR & ANDREW M. HINKES, DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY: US LAW AND REGULATION 16 (2020); DEL WRIGHT JR., A SHORT & HAPPY GUIDE TO BITCOIN, BLOCKCHAIN, AND CRYPTO 1 (2020).

³⁹ In addition to Texas, New Hampshire and Arizona have passed laws enabling a cryptocurrency strategic reserve, while Massachusetts, Ohio, and South Dakota have legislation pending at various stages. Trevor Laurence Jockims, *Led by Texas, New Hampshire, U.S. States Race to Prove They Can Put Bitcoin on Public Balance Sheet*, CNBC (Jan. 17, 2026), <https://www.cnbc.com/2026/01/17/texas-us-states-budgets-bitcoin-crypto-strategic-reserve.html?msockid=0d19d6d44ac667911bc7c5a74b3766d4>. New Hampshire has also issued a bitcoin-backed municipal bond in November 2025, and several states accept cryptocurrency as payment for taxes—including Colorado, Utah and Louisiana. *Id.*

⁴⁰ David Zaslow, *Texas Becomes First State to Make Bitcoin Reserve Purchase*, BLOCKCHAIN (Dec. 14, 2025), <https://blockchain.bakermckenzie.com/2025/12/16/texas-becomes-first-state-to-make-bitcoin-reserve-purchase/>.

executive orders on supply chain resilience in critical infrastructure sectors and even directly investing in companies deemed vital to important supply chains. This Section concludes by identifying significant weaknesses of these approaches, such as its failure to affect the critical firm-level decisions that place national infrastructure at risk. Section IV sets forth this Article’s approach to aligning incentives by explaining that the *Caremark* doctrine has always been concerned with the resilience of critical infrastructure. It provides an overview of cases spanning multiple sectors to demonstrate that cases survived dismissal when they involved both harms to the corporation *and* created risks to national critical infrastructure. It concludes by arguing that corporate directors and officers must be particularly attentive in their oversight duties when the corporations they govern provide national critical infrastructure. Section V provides a framework for corporate directors and officers to use to operationalize the *Caremark* duties that this Article identifies. This Section highlights how Bitcoin mining is a type of critical digital infrastructure and applies its framework to ensuring supply chain resilience in Bitcoin mining.

I. THE PUBLIC RISKS OF PRIVATE CONTROL: CRITICAL INFRASTRUCTURE AS A NATIONAL SECURITY PRIORITY

Many sectors supply goods and services critical to the economic and national security of the nation. This is particularly true in sectors that have been deemed by the National Security Council to provide “critical and emerging technologies”⁴¹: artificial intelligence, quantum computing, space technologies, and distributed ledger technologies (including blockchain technology), among others.⁴² These emerging technologies are quickly becoming part of the fabric of society—tools that society takes for granted, assuming the technology will remain available and in working order. Emerging technologies become digital infrastructure when these technologies blossom from a tool used by a few into a ubiquitous feature of everyday life that individuals use without thinking. Like its physical counterpart, critical digital infrastructure is subject to a government-imposed resiliency framework designed to prevent major technology outages.

Infrastructure refers to the framework, services, and facilities that everyone uses to accomplish basic aspects of commercial and personal life but that most individuals take for granted. Infrastructure operates in the background, quietly “facilitating flows of human activity and exchange across spaces and scales.”⁴³ According to the White House, *critical* infrastructure “comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or

⁴¹ THE WHITE HOUSE, NATIONAL STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGIES (Oct. 2020), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf>.

⁴² *Id.* at A-1.

⁴³ Julie E. Cohen, *Platforms, Data Infrastructures, and Infrastructure Stacks*, in GLOBAL GOVERNANCE BY DATA INFRASTRUCTURES OF ALGORITHMIC RULE (Fleur Johns, et. al., eds., 2024)(considering the intersection between data and infrastructure).

destruction would have a debilitating impact on national security, national economic security, or national public health or safety.”⁴⁴ Traditionally, critical infrastructure policy centered on the physical systems⁴⁵ that “are vital for public safety, economic security, and national security,” including “[e]nergy grids, water and wastewater systems, transportation networks, healthcare facilities, [and] communications networks.”⁴⁶

Increasingly, however, both policy leaders and corporate leaders recognize the rising importance of digital infrastructure—the digital architecture and code that provides the underlying framework necessary to support e-commerce, economic and residential development, and national security. In fact, in 2013, “Information Technology,” was designated as a critical infrastructure sector and defined to include industry, assets and services that “[p]roduce[] information technology . . . include[ing] hardware manufacturers, software developers and service providers, as well as the Internet as a key resource.”⁴⁷ The information technology that rises to the level of critical digital infrastructure includes those technologies, established and emerging, that facilitate flows of activity and exchange across digital spaces in ways that society takes for granted.⁴⁸ Take the internet as an example. Just as society expects roads and bridges to be available and in good repair so that people can go to work and school, so too does society expect the internet to be available for use at work and school. Disruption to the availability of the internet would disrupt the flow of commerce in the same way that a disruption to the availability of roads would impair commerce. Thus, both roads (transportation infrastructure) and the internet (digital infrastructure) are critical infrastructure.

To help identify the industries that build and support critical infrastructure, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) identified 16 distinct sectors as critical to the national and economic security of the country including defense industrial base, energy, financial services, food and agriculture, healthcare and public health, information technology, and transportation services.⁴⁹ The U.S. government has also provided signals about which

⁴⁴ NSM-22, *supra* note 22; *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act 1016(e) (defining critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”).

⁴⁵ K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234 (2018) (“Ordinarily when we think of infrastructure we think of physical objects, roads, and bridges.”).

⁴⁶ Department of Homeland Security, Memorandum from Alejandro N. Mayorkas, Secretary, Re: Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025), at 1 (June 14, 2024), 24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf.

⁴⁷ NIPP 2013, *supra* note 22; *reaffirmed by* NSM-22, *supra* note 22.

⁴⁸ Cohen, *supra* note 42, at 22.

⁴⁹ U.S. Cybersecurity & Infrastructure Security Agency [hereinafter CISA], Critical Infrastructure Sectors, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

emerging technologies it thinks of as critical. In October 2020, the White House Office of Science and Technology Policy published the National Strategy for Critical and Emerging Technologies (“C&ET”). The Strategy classifies critical and emerging technologies “as those technologies that have been identified and assessed by the National Security Council (NSC) to be critical, or to potentially become critical, to the United States’ national security advantage, including military, intelligence, and economic advantages.”⁵⁰ Such technologies include artificial intelligence, semiconductors, and autonomous systems.⁵¹ C&ET are quickly becoming part of the digital infrastructure⁵² that supports the modern information economy, and increasingly take on national security and economic strategic value as a result.

Given the importance of infrastructure, policymakers have taken various steps to prevent disruption to its availability and to ensure that, when disruptions do occur, the broader system of infrastructural resources is resilient enough to prevent excessive economic loss.⁵³ In particular, starting in 1998, the United States created a framework for ensuring the resilience of critical infrastructure.⁵⁴ Critical infrastructure sectors have obligations to strengthen the resilience of infrastructural resources against “all threats” and “all hazards,” which includes, a duty “to minimize disruptions of Government, social, or economic activities [from, among other things] supply chain disruptions.”⁵⁵

In this context, resilience of critical infrastructure refers to “the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions.”⁵⁶ Furthermore, corporations within each critical infrastructure sector are required to account for national priorities in their risk management strategies.⁵⁷ National priorities now

⁵⁰ *Id.* at 2.

⁵¹ White House, Press Release, *White House Office of Science and Technology Policy Releases Updated Critical and Emerging Technologies List* (Feb. 12, 2024).

⁵² Most scholars identify digital infrastructure functionally, often applying Professor Brett Frishmann’s three-criteria test for “identify[ing] and evaluat[ing] infrastructure resources functionally.” BRETT M. FRISCHMANN, *INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES* XIV (2012). Specifically, a digital technology is digital infrastructure if it: (1) “may be consumed nonrivalrously for some appreciable range of demand,” (2) “social demand for the resource is drive primarily by downstream productive activity that requires the resource as an input,” and (3) “may be used as an input into a wide range of goods and service, which may include private goods, public goods, and social goods.” *Id.*; see also Cohen, *supra* note 48 ; Carla L. Reyes & Joseph Cutler, *Ready Layer One: Functional Regulation for Blockchain Infrastructure*, 77 S. CAROLINA L. REV. (forthcoming 2026).

⁵³ See Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance* (Jan. 29, 2024) (unpublished manuscript)(discussing the history of critical infrastructure policy), <https://dcfintechweek.org/wp-content/uploads/2024/09/Paper-Genuine-DeFi-as-Critical-Infrastructure.pdf>.

⁵⁴ Presidential Decision Directive 63 (PDD-63), “Critical Infrastructure Protection” (May 22, 1998).

⁵⁵ NSM-22, *supra* note 22, at 20.

⁵⁶ *Id.*

⁵⁷ *Id.*

include maintain and improving U.S. leadership in critical and emerging technologies.⁵⁸

II. THE PROBLEM OF MISALIGNED INCENTIVES BETWEEN MARKETS AND SECURITY

Despite governmental attention to critical infrastructure, corporations routinely put it at risk when their boards and senior leadership make decisions that privilege profits and other private benefits over infrastructure resilience. For example, Boeing's lack of board oversight over airplane safety led it to make decisions that cost the lives of hundreds of passengers when its planes crashed.⁵⁹ This crash not only affected the victims and their loved ones but also endangered the broader aviation sector when the FAA grounded the fleets of national and regional airlines that used Boeing planes.⁶⁰ This disruption to the aviation sector led to thousands of cancelled and delayed flights for passengers for a period of several months.⁶¹

But corporations harm infrastructure in other ways besides introducing a dangerous product or service into the marketplace. Instead, they also threaten infrastructure by failing to ensure the availability of the particular good or service that they provide to a sector. A primary reason for this failure is a lack of supply chain resilience. Supply chain resilience “addresses the supply chain’s ability to cope with the consequences of unavoidable risk events in order to return to its original operations or move to a new, more desirable state after being disturbed.”⁶² Supply chains become resilient when those who control them invest in particular supply chain capabilities, such as flexibility, visibility, and redundancy. Flexibility refers to “the ability of an enterprise to adapt to the changing requirements of its environment and stakeholders with minimum time and effort.”⁶³ Visibility refers to the corporation’s knowledge of its suppliers and sub-suppliers that allows it to detect potential disruptions before they occur.⁶⁴ Finally, redundancy refers to “the strategic and selective use of spare capacity and inventory that can be invoked during a crisis to cope, e.g. with supply shortages or demand surges.”⁶⁵

Corporations that fail to ensure these and other resilience capabilities in their supply chains can endanger the infrastructure sectors that they support. The

⁵⁸ NSM-22, *supra* note 22, at 6.

⁵⁹ *In re The Boeing Co. Derivative Litig.*, 2021 BL 337478, at *12.

⁶⁰ Thomas Kaplan, Ian Austen, and Selam Gebrekidan, *Boeing Planes Are Grounded in U.S. After Days of Pressure*, N.Y. TIMES (Mar. 13, 2019).

⁶¹ Leslie Josephs, *American Airlines extends cancellations from grounded Boeing 737 Max to Sept. 3*, CNBC (June 19, 2019).

⁶² Uta Jüttner & Stan Maklan, *Supply chain resilience in the global financial crisis: an empirical study*, 16 SUPPLY CHAIN MGMT.: AN INT’L J. 246, 247 (2011).

⁶³ Benjamin R. Tukamuhabwaa *et. al.*, *Supply chain resilience: definition, review and theoretical foundations for further study*, INT’L J. OF PROD. RES. 1, 13 (2015).

⁶⁴ *Id.* at 14.

⁶⁵ *Id.* at 13.

challenge is that these supply chain capabilities can prove costly so that many corporations may choose not to incorporate them into their supply chains. Redundancy, in particular, may be particularly unfavored by corporations that privilege cost savings, through lean manufacturing, over maintaining spare capacity in case one of their supply sites is compromised. These corporate decisions – dictated by the marketplace – can create a national crisis in one or more infrastructure sectors.

In 2022, Abbott Nutrition closed its Michigan plant for months after the Food and Drug Administration (FDA) investigated it following four infections among infants who had consumed powdered formula from the plant.⁶⁶ The plant shutdown caused a national shortage of baby food formula because Abbott controls 40% of the U.S. infant formula market and, along with three other companies, constitutes a 90% market share for national baby formula.⁶⁷ The Michigan plant was its largest manufacturing site.⁶⁸ This market organization led to two levels of concentration. First, there was a small number of corporations providing infant baby formula – a critical component of the *food and agriculture sector*. Second, some of these corporations – like Abbott – exacerbated the risks created by market concentration by not diversifying their manufacturing sites; its infant baby formula supply chain lacked redundancy because it had insufficient alternative manufacturing sites and lacked a mitigation plan to produce specialty metabolic formulas at its other facilities.⁶⁹ Due to its lack of spare capacity, Abbott's supply chain was not flexible enough to ensure that it could adapt to meet national demand when one of its plants was shut down. As noted by multiple Congressional leaders, “[t]he extremely high levels of concentration in the infant formula market creates a serious risk to infant health if there is any disruption to a major manufacturer’s supply.”⁷⁰

In yet another example, Baxter International’s North Carolina plant had to close in 2024 due to flooding caused by Hurricane Helene, creating significant risks to the *healthcare sector*.⁷¹ The plant is responsible for the manufacture of a large share of the national supply of sterile intravenous, or IV, fluids.⁷² The plant is Baxter’s largest manufacturing site and its shutdown caused the corporation to

⁶⁶ *Justice Department investigating Abbott baby formula plant*, ASSOCIATED PRESS (Jan. 21, 2023).

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ Sarah Zimmerman, *How an Infant Formula Plant Shutdown Unraveled into a National Crisis*, *Supply Chain Dive* (May 31, 2022), <https://www.supplychaindive.com/news/timeline-infant-formula-shortage/624570/>.

⁷⁰ Letter from U.S. Senator Cory A. Booker to Honorable Thomas J. Vilsack Secretary United States Department of Agriculture (May 13, 2022), https://www.booker.senate.gov/imo/media/doc/booker_duckworth_klobuchar_lead_8_senators_in_urgng_usda_to_address_infant_formula_shortages.pdf.

⁷¹ Sarah Elbeshbishi, *Helene Damaged a Factory That Makes IV Fluids*, AP NEWS (Oct. 4, 2024), <https://www.apnews.com/article/hurricane-helene-baxter-plant-intravenous-ee62f60c70fb8e64b60c5ae9c462c2a7>.

⁷² *Id.*

restrict how much supply customers were allowed to order.⁷³ The shortage led some hospitals to delay surgeries or to start their patients on water or Gatorade instead of an IV.⁷⁴ A year earlier, Pfizer’s pharmaceutical plant in North Carolina re-started production 10 weeks after it was hit by a tornado.⁷⁵ The plant is significant because it produces anesthesia, among other drugs, and “nearly one-fourth of the sterile injectable medications Pfizer supplies to U.S. hospitals.”⁷⁶

In the *energy sector*, Colonial Pipeline suffered a ransomware attack in 2021 that forced it to shut down its pipeline, leading some commentators to conclude that “‘core elements of our national infrastructure’ remain vulnerable to cyberattack.”⁷⁷ This shutdown significantly compromised the energy sector because Colonial Pipeline supplies approximately 45% of fuel used on the East Coast.⁷⁸ Similarly, several states are investing in data centers but they lack the components to make them operational, such as transformers, circuit breakers, and high-voltage cables that carry power across regions, and steel poles that hold the network together.⁷⁹ These components are necessary to supply the data centers with electricity but they are in short supply.⁸⁰

Poor supply chain resilience not only compromises physical infrastructure but also digital infrastructure. Corporations supplying digital infrastructure rely on “data supply chains”⁸¹ to keep their products and services operational. A break in these data supply chains can cause as much chaos as a break in physical supply chains. For example, in 2025, the internet crashed when the chain of code supplying its data was disrupted because the control plane malfunctioned.⁸² In the future, corporations supplying autonomous products, blockchain technology, and artificial intelligence may similarly impose disruptions on their consumers and users if they are not vigilant about maintaining their supply chains for data.⁸³

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ Jack Hale, *Tornado-Damaged Pfizer Plant in North Carolina Restarts Production*, AP NEWS (Sept. 25, 2023), <https://www.apnews.com/article/tornado-pfizer-plant-medicine-rocky-mount-cf75a1b731559699c27cfb848d58c99b>.

⁷⁶ *Id.*

⁷⁷ Marisa Peñaloza, *Ransomware Attack Shuts Down a Top U.S. Gasoline Pipeline*, NPR (May 8, 2021), <https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline>.

⁷⁸ *Id.*

⁷⁹ Daniel Morton, *Supply-Chain Delays, Rising Equipment Prices Threaten Electricity Grid*, WTNH (Nov. 14, 2025), <https://www.wtnh.com/news/national/supply-chain-delays-rising-equipment-prices-threaten-electricity-grid/>.

⁸⁰ *Id.*

⁸¹ Reyes & Parella, *supra* note 21, at 6.

⁸² Freuler, *supra* note 20, at 2.

⁸³ *Id.*

III. ALIGNING CORPORATE INCENTIVES THROUGH PUBLIC GOVERNANCE: EXECUTIVE ACTION

Successive White House administrations have used different strategies to protect critical infrastructure by strengthening supply chains. Part A provides an overview of recent executive orders on supply chain resilience that vary in scope, objectives, and sector. Part B describes how the Trump administration is seeking to bolster supply chains for emerging technologies – such as artificial intelligence – by making direct investments in companies in exchange for a sizeable equity stake. Part C explains that these strategies are inadequate because they do not affect the types of firm-level routine decision-making that are determinative of supply chain resilience and, by extension, the security of critical infrastructure.

A. Executive Orders on Supply Chain Resilience 2021-2025

In 2021, President Biden signed Executive Order 14017—America’s Supply Chains—that recognizes that “[t]he United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security.”⁸⁴ Among its features, it ordered heads of particular agencies to report to the President on risks in supply chains for semiconductors, high-capacity batteries, critical minerals and other strategic materials (including rare earth elements), and pharmaceuticals and active pharmaceutical ingredients.⁸⁵ It also ordered heads of particular agencies to perform sectoral supply chain assessments for the following sectors: defense industrial base, public health and biological preparedness industrial base, critical sectors and subsectors of the information and communications technology (ICT) industrial base, energy sector industrial base, transportations industrial base, and production of agricultural commodities and food products.⁸⁶ The heads of agencies were also ordered to report on:

- “[T]he defense, intelligence, cyber, homeland security, health, climate, environmental, natural, market, economic, geopolitical, human-rights or forced-labor risks or other contingencies that may disrupt, strain, compromise, or eliminate the supply chain.”
- “[T]he resilience and capacity of American manufacturing supply chains and the industrial and agricultural base—whether civilian or defense—of the United States to support national and economic security, emergency preparedness, and the policy identified in section 1 of this order.”

⁸⁴ Exec. Order No. 14017, *supra* note 13.

⁸⁵ *Id.*

⁸⁶ *Id.*

- “[S]pecific policy recommendations for ensuring a resilient supply chain for the sector.”⁸⁷

In 2024, President Biden signed Executive Order 14123 – White House Council on Supply Chain Resilience – that shed light on what resilient supply chains look like: “Characteristics of resilient supply chains include greater domestic production; a diverse and agile supplier base; built-in redundancies; a reliable transportation system; secure critical infrastructure; adequate stockpiles; safe and secure data networks; reliable food systems; and a world-class, globally competitive American manufacturing base and workforce.”⁸⁸

The first Trump Administration was active in ensuring the resilience of supply chains for a number of critical infrastructure sectors.⁸⁹ More recently, in his second administration, President Trump issued an Executive Order to strengthen the healthcare sector by ensuring pharmaceutical supply chain resilience, directing the Office of the Assistant Secretary for Preparedness and Response (ASPR) to identify a list of “approximately 26 drugs that are especially critical to the health and security interests of the Nation (the critical drugs).”⁹⁰

⁸⁷ *Id.* (“Such recommendations may include sustainably reshoring supply chains and developing domestic supplies, cooperating with allies and partners to identify alternative supply chains, building redundancy into domestic supply chains, ensuring and enlarging stockpiles, developing workforce capabilities, enhancing access to financing, expanding research and development to broaden supply chains, addressing risks due to vulnerabilities in digital products relied on by supply chains, addressing risks posed by climate change, and any other recommendations.”).

⁸⁸ Exec. Order No. 14123, *supra* note 13 at 51,949 (defining “critical infrastructure” as “assets, systems, and networks, whether physical or virtual, that are so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof.”).

⁸⁹ *See, e.g.*, Executive Order 13806, *supra* note 13, at 34597 (“Modern supply chains, however, are often long and the ability of the United States to manufacture or obtain goods critical to national security could be hampered by an inability to obtain various essential components, which themselves may not be directly related to national security. Thus, the United States must maintain a manufacturing and defense industrial base and supply chains capable of manufacturing or supplying those items.”); Exec. Order 13817, *supra* note 13, at 60835 (“The United States is heavily reliant on imports of certain mineral commodities that are vital to the Nation’s security and economic prosperity. This dependency of the United States on foreign sources creates a strategic vulnerability for both its economy and military to adverse foreign government action, natural disaster, and other events that can disrupt supply of these key minerals. . . . It shall be the policy of the Federal Government to reduce the Nation’s vulnerability to disruptions in the supply of critical minerals, which constitutes a strategic vulnerability for the security and prosperity of the United States.”); Executive Order 13953, *supra* note 13, at 62539 (“I therefore determine that our Nation’s undue reliance on critical minerals, in processed or unprocessed form, from foreign adversaries constitutes an unusual and extraordinary threat, which has its source in substantial part outside the United States, to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with that threat. . . . By expanding and strengthening domestic mining and processing capacity today, we guard against the possibility of supply chain disruptions and future attempts by our adversaries or strategic competitors to harm our economy and military readiness.”).

⁹⁰ ENSURING AMERICAN PHARMACEUTICAL SUPPLY CHAIN RESILIENCE BY FILLING THE STRATEGIC ACTIVE PHARMACEUTICAL INGREDIENTS RESERVE, Executive Order No. 14336, 90 Fed. Reg. 40223 (Aug. 19, 2025).

Subject to funding, the ASPR “shall obtain a 6-month supply of the [active pharmaceutical ingredients] needed to make the critical drugs to fill the Strategic Active Pharmaceutical Ingredients Reserve].”⁹¹

On December 6, 2025, the White House adopted a strategy to strengthen the food and agriculture sector by creating a Food Supply Chain Security Task Force within the Department of Justice and the Federal Trade Commission to investigate whether “anti-competitive behavior exists in food supply chains in the United States, as well as whether control of food-related industries by foreign entities is increasing the cost of food products in the United States or creating a national or economic security threat to Americans.”⁹²

B. “Executive Shareholderism”: Building Supply Chain Resilience Through Government Equity Stakes in Companies

In 2025, the White House adopted another strategy to strengthen the supply chains supporting critical *digital* infrastructure by taking a 10%-15% equity stake in over half a dozen companies: Intel Corporation, MP Materials, Lithium Americas Corporation, Trilogy Materials Inc., Vulcan Elements, and xLight. All of these companies produce goods and services critical to the supply chains of critical and emerging technologies.

On July 10, 2025 MP Materials announced that it had entered into a public-private partnership with the U.S. Department of Defense that, among other things, includes a significant equity stake in the company. MP Materials is the largest producer of rare earth materials in the U.S. with the ability to perform mining and processing to advanced metallization and magnet manufacturing.⁹³ The U.S. will invest in MP Materials to build up the domestic industrial base for rare earth magnets so that the U.S. can reduce its dependence on foreign sources.⁹⁴

On August 22, 2025, Intel Corporation announced that the U.S. government would take a \$8.9 billion investment in Intel’s common stock.⁹⁵ Intel is critical to the U.S. semiconductor manufacturing sector because it operates a foundry

⁹¹ *Id.*

⁹² Exec. Order of Dec. 6, 2025, *supra* note 13.

⁹³ MP Materials Corp., *Investor Relations Overview*, MP MATERIALS (last visited Feb. 7, 2026), <https://investors.mpmaterials.com/overview/default.aspx>.

⁹⁴ MP Materials Corp., Press Release, *MP Materials Announces Transformational Public-Private Partnership With the Department of Defense to Accelerate U.S. Rare Earth Magnet Independence* (July 10, 2025), <https://mpmaterials.com/news/mp-materials-announces-transformational-public-private-partnership-with-the-department-of-defense-to-accelerate-u-s-rare-earth-magnet-independence/>.

⁹⁵ Intel Corp., Press Release, *Intel and Trump Administration Reach Historic Agreement to Accelerate American Technology and Manufacturing Leadership* (Aug. 22, 2025), <https://www.intc.com/news-events/press-releases/detail/1748/intel-and-trump-administration-reach-historic-agreement-to>.

business as a chip maker.⁹⁶ Chips are critical to the national security race for dominance in critical and emerging technologies, such as artificial intelligence and quantum computing. According to Intel's press release, the government will purchase 433.3 million primary shares of Intel common stock at a price of \$20.47 per share, which is approximately a 10% stake in Intel.⁹⁷ The government paid for its investment through previous grants awarded under the U.S. CHIPS and Science Act and the Secure Enclave program.⁹⁸

On October 1, 2025, the U.S. Department of Energy announced that it was investing in the lithium supply chain by restructuring a previous loan made to Lithium Americas Corporation (LAC) in exchange for a 10% equity stake.⁹⁹ The revised terms provide the government with 5% equity ownership through LAC warrants and an additional 5% ownership through warrants in a joint venture between LAC and General Motors.¹⁰⁰

Trilogy Materials is a metal exploration and development company with a 50% stake in a joint venture that owns a valuable critical minerals projects in Alaska.¹⁰¹ In October 2025, Trilogy Metals announced a binding letter of intent with the U.S. Department of War with the latter investing \$35.6 million for the development of critical mineral resources in the Alaskan projects.¹⁰² In exchange, the Department of War will receive a 10% stake in Trilogy Materials and "shall have the right to appoint one independent third-party director to the board of directors of Trilogy Metals for a period of three years."¹⁰³

Vulcan Elements is a manufacturer of rare earth magnets.¹⁰⁴ In November 2025, the Office of Strategic Capital, within the U.S. Department of War, announced "a joint \$700 million conditional loan commitment with Vulcan Elements [] and

⁹⁶ Katie Tarasov, *Intel Aims to Find Clients and Catch TSMC With New Chip Fab in Arizona*, CNBC (Dec. 19, 2025), <https://www.cnbc.com/2025/12/19/intel-aims-to-find-clients-and-catch-tsmc-with-new-chip-fab-in-arizona.html>.

⁹⁷ Intel Corp., Press Release, *supra* note 94.

⁹⁸ *Id.* ("The government's equity stake will be funded by the remaining \$5.7 billion in grants previously awarded, but not yet paid, to Intel under the U.S. CHIPS and Science Act and \$3.2 billion awarded to the company as part of the Secure Enclave program. Intel will continue to deliver on its Secure Enclave obligations and reaffirmed its commitment to delivering trusted and secure semiconductors to the U.S. Department of Defense. The \$8.9 billion investment is in addition to the \$2.2 billion in CHIPS grants Intel has received to date, making for a total investment of \$11.1 billion.").

⁹⁹ U.S. Dep't of Energy, Press Release, *Department of Energy Restructures Lithium Americas Deal to Protect Taxpayers and Onshore Critical Minerals* (Oct. 1, 2025), <https://www.energy.gov/articles/department-energy-restructures-lithium-americas-deal-protect-taxpayers-and-onshore>.

¹⁰⁰ *Id.*

¹⁰¹ Trilogy Metals, Press Release, *Trilogy Metals Announces Strategic Investment by US Federal Government* (Oct. 6, 2025), <https://trilogymetals.com/news-and-media/news/trilogy-metals-announces-strategic-investment-by-us-federal-government/>.

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ Vulcan Elements, *Home, Vulcan Elements* (last visited Feb. 7, 2026), <https://vulcanelements.com/>.

ReElement Technologies [] to increase domestic Neodymium Iron Boron (NdFeB) magnet production and significantly bolster U.S. critical minerals supply chains.”¹⁰⁵ Per the commitment, “[t]hese loans will directly support the production of advanced rare earth element separation, metallization, and magnet manufacturing capabilities in the United States.”¹⁰⁶ The loan was justified as a way to strengthen U.S. supply chains for the magnets used in a wide variety of application, including chip manufacturing.¹⁰⁷

xLight is a start-up that aims to aid semiconductor manufacturing by producing a new light source that can assist lithography, a critical component of chip manufacturing.¹⁰⁸ On December 1, 2025, the Department of Commerce’s CHIPS Research and Development Office announced that it signed a nonbinding letter of intent (LOI) with xLight to award it \$150 million under the CHIPS Act.¹⁰⁹ According to the press release, the “potential incentives would be for the construction, build out, and demonstration of a free-electron laser (FEL) prototype as an alternative light source for extreme ultraviolet (EUV) lithography.” In exchange, the Department of Commerce would receive \$150 million of equity in xLight.¹¹⁰

C. *Limitations of Executive Actions*

Both types of executive action can strengthen supply chains supporting a variety of different sectors. However, on their own, they are unlikely to ensure effective resilience of critical supply chains because they do not target the firm-level corporate decision-making that can lead to supply chain vulnerabilities.

¹⁰⁵ U.S. Dep’t of War, Press Release, *Office of Strategic Capital Agrees to Joint \$700M Conditional Loan Commitment with Vulcan Elements and ReElement Technologies* (Nov. 21, 2025).

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ xLight Inc., *Home*, xLight (last visited Feb. 7, 2026), <https://www.xlight.com>.

¹⁰⁹ National Institute of Standards and Technology, Press Release, *Department of Commerce and NIST Announce CHIPS Research and Development Letter of Intent with xLight, Inc. for Extreme Ultraviolet Lithography* (Dec. 1, 2025) (last visited Feb. 7, 2026), <https://www.nist.gov/news-events/news/2025/12/department-commerce-and-nist-announce-chips-research-and-development-letter>

¹¹⁰ *Id.* But it is not only the executive branch that is seeking to strengthen U.S. supply chains for critical infrastructure. In November 2025, U.S. Senators Jim Banks, Elizabeth Warren, Tom Cotton, Chris Coons, Dave McCormick, and Chuck Schumer introduced a bipartisan bill – the Guaranteeing Access and Innovation for National Artificial Intelligence (GAIN AI) Act – that “would require companies to give American businesses first priority in acquiring advanced AI chips before exporting these chips to China and other countries of concern.” U.S. Senate Committee on Banking, Housing, and Urban Affairs, Press Release, Banks, Warren, Cotton, Schumer, McCormick, Coons Introduce Landmark Bipartisan GAIN AI Act to Maintain U.S. Position As World’s Leader in Critical Artificial Intelligence Chips (Nov. 7, 2025). According to the bill’s sponsors, “[o]nly after fulfilling purchases from U.S.-based customers could a company export their chips to countries of concern, assuming such sales are permitted under U.S. export controls.” *Id.*

The executive orders direct federal agencies to take particular actions, such as collecting information or investigating potential misconduct by industry actors. But these executive orders seek to change *government* conduct, not industry conduct. Specifically, their objectives include improving interagency efforts to ensure supply chain resilience;¹¹¹ detecting supply chain risks in critical infrastructure sectors;¹¹² identifying contingencies that may compromise critical supply chains and assess capabilities to respond;¹¹³ recommending legislative, regulatory and policy changes as needed;¹¹⁴ directing interagency coordination on strengthening supply chains for critical minerals;¹¹⁵ assessing and reporting on national reliance on foreign adversaries for critical minerals;¹¹⁶ ensuring supply of active pharmaceutical ingredients;¹¹⁷ and investigating potential misconduct by industry actors and foreign adversaries in food supply chain,¹¹⁸ among other strategies. These various supply chains aim to bolster the *national* supply chains through enhanced reporting, assessment, and contingency planning so that the federal government has an aggregate view of national supply chain vulnerabilities in particular sectors. But, by adopting a systems level perspective, it neglects the defects at the firm-level: supply chain vulnerabilities in the individual supply chains governed by corporations and other businesses.

Direct investment allows the federal government to engage with corporate supply chains on a granular level. Equity holders are traditionally afforded certain types of governance rights not extended to general public, such information rights and voting rights.¹¹⁹ But, even as equity holders, the federal government may lack the type of governance rights that would enable it to ensure supply chain resilience. First, the investment agreements between the federal agencies and the affected companies limit the government's ability to exercise governance rights, even indirectly. For example, while owning a sizable stake in Intel, the government agreed that it would have neither information rights nor representation on Intel's board of directors nor other governance rights.¹²⁰ It also "agrees to vote with [Intel's] Board of Directors on matters requiring shareholder approval, with limited exceptions."¹²¹ In contrast, the Department of War has the right to appoint an independent third-party director

¹¹¹ Exec. Order No. 14123 § 4, *supra* note 13.

¹¹² Exec. Order No. 14017 § 3, *supra* note 13.

¹¹³ Exec. Order No. 13806 § 2, *supra* note 13.

¹¹⁴ *Id.*

¹¹⁵ Exec. Order No. 13817 § 4, *supra* note 13.

¹¹⁶ Executive Order 13953 § 1, *supra* note 13.

¹¹⁷ Executive Order 14336, 90 § 2, *supra* note 13.

¹¹⁸ Exec. Order of Dec. 6, 2025, *supra* note 13.

¹¹⁹ See, e.g., FRANK PARTNOY & ELIZABETH POLLMAN, BUSINESS ORGANIZATIONS: A CONTEMPORARY APPROACH 557 (2023) (explaining that shareholders "exercise their limited corporate governance role mostly by voting" on elections of the corporate directors; certain fundamental transactions; amendments to the articles of incorporation, among other matters).

¹²⁰ Intel Corp., Press Release, *supra* note 94 ("The government's investment in Intel will be a passive ownership, with no Board representation or other governance or information rights.").

¹²¹ *Id.*

to the board of directors of Trilogy Metals for a period of three years.¹²² It is not unprecedented for the federal government, through its agencies, to have extensive control and governance rights over particular companies but these are generally limited to particular situations, such as government contractors subject to foreign ownership, control, or influence.¹²³ There is no publicly available information that suggests that the federal agencies have comparable governance rights over the companies discussed above.

Second, even if the agreements provide the federal government with governance rights, the agencies, as equity holders, are unlikely to have a vote on supply chain management issues, such as evaluation and selection of suppliers; design of supply chain contracts; investment, planning and development of manufacturing capacity; and allocation of manufacturing capacity. These day-to-day decisions would be the prerogative of corporate management. Even the Department of War – possessing the right to appoint a director to Trilogy Metals’s board – is unlikely to affect supply chain resilience meaningfully because these supply chain matters frequently do not rise to the level of the board. According to experts, corporate boards routinely neglect supply chain management even when supply chains pose risks to the corporation.¹²⁴ Under these circumstances, federal agencies would only be able to direct the companies’ supply chain choices if they inserted their own employees into management positions or required the companies to make prescribed supply chain choices. Either approach would involve the federal government in the internal decision making of individual companies – an unusual posture in American capitalism that risks eroding the traditional and valued boundary between state and industry.

Collectively, neither type of executive strategy incentivizes corporate management to prioritize supply chain resilience over profits or other private interests. The consequence is that their supply chains may lack the redundancy, flexibility, and visibility required to prevent a threat to critical infrastructure or to address it once it materializes.

¹²² *Id.*

¹²³ Verstein, *supra* note 25, at 798 (“Complying companies are often required to recruit one or more ‘outside’ directors to the board. An Outside Director ‘acts on behalf of the US government.’”)] The mitigation agreement asserts that it preempts any state law fiduciary duties to the company and its shareholders that Outside Directors would otherwise owe.]] Instead, they may satisfy those duties only ‘in a manner believed to be in the U.S. national interest.’”) (citations omitted).

¹²⁴ See, e.g., Steven Lustig, *How Public Company Boards Can Mitigate Supply Chain Risk*, DIRECTORS & BOARDS (May 24, 2023) (“Unfortunately, few board members currently provide expertise in supply chain management and the associated risk mitigation.”); Timothy J. Pettit, Joseph Fiksel & Keely L. Croxton, *Ensuring Supply Chain Resilience: Development of a Conceptual Framework*, 31 J. BUS. LOGISTICS 1 (2010) (“[T]raditional risk management techniques are lacking in their ability to assess the complexities of supply chains, evaluate the intricate interdependencies of threats, and prepare an enterprise for the unknowns of the future.”).

IV. ALIGNING CORPORATE INCENTIVES THROUGH PRIVATE GOVERNANCE: THE *CAREMARK* APPROACH

The nation's supply chains are in the hands of individual companies. The inability of these companies to manage the supply chain—and their resulting failure to deliver their goods and services—not only harms shareholders but also the economic and national security priorities of the country.

This Article argues that directors and officers of corporations supplying critical infrastructure should prioritize supply chain resilience as part of the oversight duties developed by *In re Caremark*¹²⁵ and its subsequent cases. Those cases explained that “[w]here directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.”¹²⁶ *Stone v. Ritter* further clarified that directors can be subject to this oversight liability if they failed either of these two prongs: “(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.”¹²⁷

As Part A explains, many of the *Caremark* cases that have survived dismissal share an important feature: the oversight failures of the corporate managers harmed both the companies they govern but also created risks to one or more critical infrastructure sectors of the United States.¹²⁸ Part B uses this case review to argue that management of corporations providing critical infrastructure must ensure the resilience of supply chains as part of the *Caremark* duty that emerges from these cases. Crucially, this is not an expansion of *Caremark*'s scope to address new challenges. Instead, it has always been the rule – just largely unrecognized.

¹²⁵ *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996); *Marchand v. Barnhill*, 212 A.3d 805, 823 (Del. 2019).

¹²⁶ *Stone v. Ritter*, 911 A.2d at 362, 370.

¹²⁷ *Id.*; see also *In re The Boeing Co. Derivative Litig.*, 2021 BL 337478, at *27 (Del. Ch. Sept. 07, 2021) (“Directors may use their business judgment to ‘design context-and industry-specific approaches tailored to their Companies’ businesses and resources. But *Caremark* does have a bottom-line requirement that is important: the board must make a good faith effort—i.e., try—to put in place a reasonable board-level system of monitoring and reporting.’” [¶] This oversight obligation is ‘designed to ensure reasonable reporting and information systems exist that would allow directors to know about and prevent wrongdoing that could cause losses for the Company.’ [¶] ‘[O]nly a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability.’”) (citations omitted).

¹²⁸ *Ontario Provincial Council of Carpenters' Pension Tr. Fund v. Walton (Walmart Laches)*, 2023 WL 2904946, at *18 (Del Ch. Apr. 12, 2023) (“[T]here will be a period of time (perhaps prolonged) marked by a combination of inaction and occasional action, followed by a corporate trauma in which the corporation suffers substantial harm.”).

A. Caremark Has Always Been About Critical Infrastructure

Understanding *Caremark* oversight duties as national security strategy requires starting at the moment the duties entered corporate governance doctrine. Namely, the cases that defined the contours of the *Caremark* duties themselves—*Caremark* and *Ritter*—involved compliance failures related to critical infrastructure. *Caremark* itself involved failure to identify, prevent, or put an end to a Medicare and Medicaid kickback scheme – firm-level compliance failures related to the nation’s healthcare infrastructure.¹²⁹ *Stone v Ritter*, for its part, centered on a financial institution’s failure to adequately comply with the Bank Secrecy Act’s requirements to combat money laundering,¹³⁰ thereby failing to adequately safeguard against a threat to the nation’s financial infrastructure. *Caremark* claims have not strayed from their origins at all: the cases that have most successfully asserted *Caremark* claims involved compliance failures related to critical infrastructure. This Section reviews these cases by examining them through the lens of critical infrastructure with national security importance.

1. Food and Agriculture

Marchand v. Barnhill involved a shareholder lawsuit against the directors and executives of Blue Bell Creameries USA, Inc., “one of the country’s largest ice cream manufacturers.”¹³¹ It experienced a listeria outbreak in 2015, “causing the company to recall all of its products, shut down production at all of its plants, and lay off over a third of its workforce.”¹³² Its failure to contain the listeria outbreak in its manufacturing plants led to the death of three people.¹³³ Blue Bell Creameries operates in the food and agricultural sector and, as such, the court noted that it was subject to significant regulation.¹³⁴ Government regulators had found compliance failures at a number of Blue Bell’s facilities.¹³⁵ The complaint survived a motion to dismiss because sufficient facts existed to cast doubt on the existence of any Board-level compliance and monitoring system.¹³⁶ The court went on to explain that “[w]hen a plaintiff can plead an inference that a board has undertaken no efforts to make sure it is informed of a compliance issue intrinsically critical to the company’s business operation, then that supports an inference that the board has not made the good faith effort that *Caremark* requires.”¹³⁷ The court’s opinion makes it clear that the board’s neglect endangered the operations of the company, thereby demonstrating firm-level

¹²⁹ *In re Caremark Int’l Inc. Derivative Litig.*, 698 A.2d at 962-63.

¹³⁰ *Stone v. Ritter*, 911 A.2d at 365.

¹³¹ *Marchand v. Barnhill*, 212 A.3d 805, 807 (Del. 2019).

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.* at 810 (“As a U.S. food manufacturer, Blue Bell operates in a heavily regulated industry.”).

¹³⁵ *Id.* at 811-812.

¹³⁶ *Id.* at 822 (“[T]he complaint supports an inference that no system of board-level compliance monitoring and reporting existed at Blue Bell”).

¹³⁷ *Id.*

harm. But it is also worth noting that Blue Bell is a food company whose products are ingested by the public. Moreover, the compliance failures related to the national systems created to protect a critical industrial sector: food production.¹³⁸ As such, its food safety is a matter of national concern even if its particular product—ice cream—may not be deemed as a critical staple of the American diet. When a board fails to oversee compliance with regulations designed to safeguard a critical infrastructure sector—here, the food and agriculture sector¹³⁹—*Caremark* duties enable private enforcement of the national security interest in maintaining the availability and good working order of key national infrastructure.¹⁴⁰

2. Healthcare and Public Health

In re Clovis is an even more stark example of the public infrastructural harm that results from a failure of board oversight. Clovis Oncology, Inc. is a biopharmaceutical company that “focused on acquiring, developing and commercializing cancer treatments.”¹⁴¹ The lawsuit concerned a cancer drug in development that was undergoing FDA clinical trials and that was “designed to treat a previously-untreatable type of lung cancer.”¹⁴² The shareholder lawsuit alleged that the board knew that Clovis was departing from the established protocols for the clinical trial – departures that would result in the FDA denying approval for the drug.¹⁴³ The issue was how Clovis was calculating the success of the drug – its objective response rate (ORR)—during the clinical trial.¹⁴⁴ The

¹³⁸ CISA, *Food & Agriculture Sector*, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector> (last visited Feb. 5, 2026).

¹³⁹ *Id.*

¹⁴⁰ Other claims of *Caremark* duty violations related to the food and agricultural sector have similarly survived the motion to dismiss stage. *See, e.g., In re Abbott Laboratories Infant Formula Shareholder Deriv. Litig.* No. 22-CV-05513 (N.D. Ill. Aug. 7, 2024) (allowing *Caremark* claims to move past motion to dismiss); *Lashkari v. Chipotle Mexican Grill, Inc., et al.*, 1:16-cv-03180-WJM-KLM, Order Approving Derivative Action Settlement (D. Colo. Apr. 4, 2018) (approving a settlement requiring corporate governance reforms after plaintiffs allegations of duty of loyalty violations led to a series of food borne illness outbreaks at Chipotle locations).

¹⁴¹ *In re Clovis Oncology, Inc. Derivative Litig.*, 2019 BL 373697, at *4.

¹⁴² *Id.* at *2.

¹⁴³ *Id.* at *4 (“To obtain FDA approval, new drugs like Roci and Tagrisso must prove their efficacy and safety in clinical trials. [] Before commencing a clinical trial, the FDA requires a drug’s sponsor to agree to certain standards that define how the trial will be conducted, how the trial data will be analyzed and, most relevant here, how success in the trial will be measured. [] These agreed-upon standards become the ‘clinical trial protocol.’ [] If the drug’s sponsor fails to adhere to the clinical trial protocol, the FDA will not approve a new drug for market.”) (citations omitted).

¹⁴⁴ *Id.* at *5. The complaint alleged that the board of Clovis received reports “suggest[ing] that, while the clinical trial protocol required Clovis to calculate ORR based only on confirmed responses, Clovis was actually calculating ORR, in part, based on unconfirmed responses.” *Id.* “Despite these public signals, as early as June 12, 2014, the Board received reports indicating Clovis was improperly calculating Roci’s [objective response rate]. [] Specifically, these reports suggested that, while the clinical trial protocol required Clovis to calculate [objective response

board was also aware that Clovis's management was publicly reporting the drug's success rate in the clinical trials using unconfirmed responses—a violation of the clinical trial protocol.¹⁴⁵ They were also aware that management continued to represent publicly that its drug's success was just as good (or even better) than the success rate of its competitor's drug that was also under consideration for FDA approval.¹⁴⁶ The board was also aware that management was publicly misreporting the side-effects of the drug and that the “FDA identified a failure to report two serious adverse events, approximately twelve patient eligibility violations and various failures to maintain case history and informed consent records.”¹⁴⁷

The court had no trouble identifying the ways that the board's neglect endangered the company: “ORR was the crucible in which Roci's safety and efficacy were to be tested. Roci was Clovis' mission critical product.”¹⁴⁸ But the board's mismanagement also endangered the public because the facts suggest that the FDA was only going to approve one of the cancer drugs undergoing development—either Clovis's or the one developed by its competitor, AstraZeneca.¹⁴⁹ The latter's result was based on confirmed responses—as required by the clinical trial—which were stronger than Clovis's.¹⁵⁰ Had Clovis not been caught, there is a risk that the FDA would have approved the less effective drug—Clovis'—and prevented or delayed the more effective competitor drug from reaching the market. As such, the board's oversight failures directly endangered the national supply of cancer drugs for a type of lung cancer that was previously untreatable. Once again, this case's survival of dismissal involves both harms to the company and to the nation's critical infrastructure – the healthcare sector.

rate] based only on confirmed responses, Clovis was actually calculating [objective response rate], in part, based on unconfirmed responses.” *Id.* (citations omitted).

¹⁴⁵ *Id.* at *5-*6 (“With hands on their ears to muffle the alarms, on February 27, 2015, Defendants Mahaffy, Mast, Atwood, Barrett, Blair, Flaherty, Graham, Klingenstein, McKinley and Spickschen signed Clovis' 2014 Annual Report. [] The report reaffirmed previous, inflated ORR reports and omitted that Clovis was relying on partially unconfirmed responses.”).

¹⁴⁶ *Id.* at *5 (“Mindful of the race to market, Clovis' management consistently represented that Roci's [objective response rate] was at least as encouraging as Tagrisso's. . . . Roci was Clovis' champion and it was prepared to do battle with Tagrisso. On September 9, 2014, Mahaffy told a securities analyst that Roci and Tagrisso had ‘similar response rate[s],’ and on November 18, 2014, Clovis issued a press release stating that Roci's ORR was 67%.”).

¹⁴⁷ *Id.* at *7-*8.

¹⁴⁸ *Id.* at *12.

¹⁴⁹ *Id.* at *4 (As the Roci clinical trial began, the Board knew time was of the essence. AstraZeneca's competing drug, Tagrisso, was also in the race for FDA approval.”).

¹⁵⁰ *Id.* at *6 (“As the Company was touting Roci's prospects, management gave a presentation to the Board explicitly comparing Roci's 63% mixed ORR to Tagrisso's confirmed 70%.”); *id.* (“At the same time, management presented a slide to the Board to illustrate how Roci was stacking up against Tagrisso. [] The slide clearly showed an [objective response rate] of 46% that was ‘(Unconf + Conf)’ while Tagrisso's ORR was ‘Confirmed.’”).

Other cases have also proven successful at the pleading stage when they similarly involved risk to the stability of the public health and healthcare sector.¹⁵¹ For example, the Delaware Court of Chancery allowed two of three claims against Walmart to move forward on theories of *Caremark* violations when Walmart's compliance with pharmaceutical regulations came under fire.¹⁵² Similarly, the Delaware Supreme Court determined that the dismissal of claims against AmerisourceBergen Corporation for failure to monitor compliance with pharmaceutical regulations was an error, and remanded the case for further proceedings.¹⁵³ In each of these cases against Clovis, Walmart, and AmerisourceBergen, the shareholders sought to vindicate harm to the corporation suffered as a result of a corporate trauma that threatened the stability of a much larger critical infrastructure sector. The high threshold for *Caremark* liability standard is met more often than in other contexts when the company operates in a critical infrastructure sector and utterly fails to monitor for, ignores, or intentionally violates regulations designed to protect the availability, stability, and good working order of critical infrastructure.¹⁵⁴

3. Transportation Systems

Boeing is a “global aerospace corporation that designs, manufactures, and sells commercial airplanes and other aviation equipment for the airline, aerospace, and defense industries.”¹⁵⁵ Its commercial aircraft business falls within the

¹⁵¹ See, e.g., *Guiliano v. Grenfell-Gardner*, C.A. No. 2021-0452-KSJM, 2025 WL 250176, at *11 (Del. Ch. 2025) (court denied motion to dismiss *Caremark* claims against a pharmaceutical company, saying “[p]laintiff adequately alleges at least a red-flags claim against Grenfell-Gardner and Richardson. Just as it is reasonably conceivable that the Board failed to receive notice of red flags, it is reasonably conceivable that Grenfell-Gardner and Richardson were aware of the red flags and failed to report them to the Board.”); *Ontario Provincial Council of Carpenters’ Pension Trust Fund, et al. v. Walton, et al.*, C.A. No. 2021-0827-JTL (Del. Ch. Apr. 26, 2023) (denying motion to dismiss some *Caremark* claims involving Walmart’s pharmacies); *Lebanon County Employees’ Retirement Fund v. Collis*, No. 22, 2023 (Del. Dec. 18, 2023) (reversing the granting of a motion to dismiss against a pharmaceutical company).

¹⁵² See, e.g., *Ontario Provincial Council of Carpenters’ Pension Tr. Fund v. Walton et al.*, C.A. No. 2021-0827-JTL (allowing claims on two of three allegations that Walmart directors failed to properly monitor and oversee compliance with regulatory requirements imposed upon its more than 5,000 pharmacies to move forward, whether under *Caremark* or Massey theories of the case).

¹⁵³ *Lebanon County Employees’ Retirement Fund v. Collis*, No. 22, 2023 (Del. Dec. 18, 2023) (reversing the Delaware Chancery decision that dismissed *Caremark* and *Massey* claims against AmerisourceBergen Corporation for failure to monitor compliance and failing to comply with regulations applicable to opioid distribution through its pharmacies, and instead allowing the claims to move forward).

¹⁵⁴ Notably, even if the company operates in a critical infrastructure sector like healthcare, if the corporate harm does not threaten the stability of the critical infrastructure, the claims are less likely to survive dismissal. For example, when Walgreens shareholders sued over billing issues, the case was dismissed. *Clem v. Skinner*, 2024 WL 668523 (Del. Ch. Feb. 19, 2024). Although Walgreens is a pharmacy and part of the healthcare and public health critical infrastructure sector, the compliance violations did not impact the stability of the system, just the stability of Walgreen’s profits.

¹⁵⁵ *In re The Boeing Co. Derivative Litig.*, 2021 BL 337478, at *2 (Del. Ch. Sept. 07, 2021).

critical infrastructure sector of transportation systems (aviation) and defense industrial base. In 2018 and 2019, two aircraft manufactured by Boeing—the 737 MAX—crashed, killing everyone on board the aircraft.¹⁵⁶ In denying dismissal, the Delaware Court of Chancery documented all of the ways that Boeing’s board did not prioritize airplane safety, including that Boeing’s Audit Committee’s charter did not include airplane safety and, as a result, the record does not indicate that the committee regularly or effectively discussed airplane safety.¹⁵⁷ The board, as a whole, also routinely failed to discuss airplane safety: “The Board did not regularly allocate meeting time or devote discussion to airplane safety and quality control until after the second crash. Nor did the Board establish a schedule under which it would regularly assess airplane safety to determine whether legitimate safety risks existed.”¹⁵⁸

This is puzzling for two reasons. First, Boeing was in a heavily regulated industry and the safety of its aircraft was “essential and mission critical” to Boeing’s business.¹⁵⁹ A failure to do so created firm-level harms for the company. But the inattention to airplane safety led to the deaths of those who travel on Boeing’s aircraft. Second, Boeing is a major U.S. manufacturer of large commercial jet liners used by domestic airlines. Its failure to oversee airplane safety has knock on effects for the national aviation industry. The FAA grounded the entire Boeing 737 MAX fleet in March, 2019.¹⁶⁰ The FAA did not clear the 737 MAX to fly until late 2020.¹⁶¹ Boeing’s airline clients – United Airlines, American Airlines and Southwest Airline – also cancelled hundreds of daily flights because they could not use the Boeing 737 MAX jets in their fleets.¹⁶² All of this demonstrates that the failure of oversight by Boeing’s boards

¹⁵⁶ *Id.* at *12 (“On October 29, 2018, a new 737 MAX flying as Lion Air Flight 610 crashed in the Java Sea minutes after taking off from Jakarta, Indonesia, killing all 189 passengers and crew.”); *id.* at *17 (“On March 10, less than one month after the Board declined to pursue an internal investigation, another 737 MAX crashed. Ethiopian Airlines Flight ET 302 went down shortly after taking off, killing all 157 passengers and crew. The pilots followed Boeing’s recommended emergency procedures, but could not regain control of the plane because MCAS repeatedly activated.”).

¹⁵⁷ *Id.* at *5 (“Boeing did not implement or prioritize safety oversight at the highest level of the corporate pyramid. None of Boeing’s Board committees were specifically tasked with overseeing airplane safety, and every committee charter was silent as to airplane safety.”); *id.* at *29 (“The Amended Complaint alleges the Board had no committee charged with direct responsibility to monitor airplane safety. While the Audit Committee was charged with “risk oversight,” safety does not appear in its charter. Rather, its oversight function was primarily geared toward monitoring Boeing’s financial risks.”).

¹⁵⁸ *Id.* at *28.

¹⁵⁹ *Id.*

¹⁶⁰ Thomas Kaplan, Ian Austen & Selam Gebrekidan, *Boeing Planes Are Grounded in U.S. After Days of Pressure*, N.Y. TIMES (Mar. 13, 2019).

¹⁶¹ Andrew Tangel & Andy Pasztor, *Boeing 737 MAX Cleared to Fly Again, but Covid-19 Has Sapped Demand*, WALL ST. J. (Nov. 18, 2020).

¹⁶² See Leslie Josephs, *American Airlines extends cancellations from grounded Boeing 737 Max to Sept. 3*, CNBC (June 19, 2019) (reporting that American Airlines cancelled 115 flights per day); Dawn Gilbertson, *Southwest canceling nearly 400 daily summer flights due to 737 Max: What travelers need to know*, USA TODAY (Feb. 13, 2020) (“Southwest said it will proactively cancel 371 daily summer flights from its schedule of more than 4,000 flights to cover the loss of the Max through

creates harms that extend well beyond Boeing's shareholders and even those directly affected by the loss of life that the crashes caused. Instead, the board's neglect compromised the nation's aviation transportation systems.

4. Energy

Shareholders of Massey Energy Co. brought several derivative lawsuits against the company's directors after a mine explosion in April 2010 claimed twenty-nine lives.¹⁶³ The disaster caused such irreparable harm to the company's reputation that the company's stock fell precipitously and the company was later sold to a competitor.¹⁶⁴ The shareholders styled their claim as a *Caremark* claim, alleging that the directors utterly failed to heed numerous red flags that signaled their mining practices were unsafe and in violation of law.¹⁶⁵ In evaluating the veracity of the plaintiffs' *Caremark* claims, the Delaware Court of Chancery emphasized plaintiffs' particularized allegations that the mine explosion and other mining safety violations were caused by an intentional strategy Massey Energy adopted.¹⁶⁶ The directors intentionally chose to disobey law in order to pursue a higher profit margin, putting their employees, the environment, and ultimately the stability of several important natural resource mines at risk.¹⁶⁷ Ultimately, the Massey Energy directors were found to have breached their duty of loyalty by intentionally violating a known law – not for failing to implement a monitoring and oversight system or ignoring red flags.¹⁶⁸

Aug. 10.”); Alison Sider, *United Airlines Removes MAX From Schedules Until June*, WALL ST. J. (Dec. 20, 2019) (“The grounding has stretched on longer than most carriers anticipated, forcing airlines to remake schedules month after month and cancel thousands of flights. The carrier said it would have to cancel some 11,520 flights due to the MAX’s absence next year, including the latest delay. United had 14 MAX jets in its fleet at the time of the grounding. The Chicago-based carrier expected to have 30 by the end of this year and to receive another 28 in 2020.”).

¹⁶³ *In re Massey Energy Company*, C.A. No. 5430-VCS, at *1 (Del. Ch. May 31, 2011) (“The plaintiffs are stockholders of Massey Energy Company, a coal mining corporation with a controversial reputation. . . . On April 5, 2010, a massive explosion occurred at Massey’s Upper Big Branch mine in West Virginia and as a result, 29 miners died.”).

¹⁶⁴ *Id.* (“In the wake of the disaster, Massey’s stock price fell dramatically and its shares were arguably trading at a discount to its coal reserves in comparison to its competitors who were not under a regulatory cloud. . . . Massey’s ‘Board,’ . . . entered into a ‘Merger Agreement’ with Alpha Natural Resources, Inc., a mining company with a good reputation and track record for miner safety and regulatory compliance.”).

¹⁶⁵ *Id.* at *19 (“The plaintiffs acknowledge that the Derivative Claims center of the allegation that directors and officers of Massey breached their fiduciary duties by failing to make a good faith effort to ensure that Massey complied with applicable laws designed to protect the safety of miners.”).

¹⁶⁶ *Id.*

¹⁶⁷ *Id.* at *20 (“Delaware law does not charter law breakers. Delaware law allows corporations to pursue diverse means to make a profit, subject to a critical statutory floor, which is the requirement that Delaware corporations only pursue ‘lawful business’ by ‘lawful acts.’”).

¹⁶⁸ *Ontario Provincial Council of Carpenters’ Pension Tr. Fund v. Walton et. al.*, C.A. No. 2021-0827-JTL at 70 (“A Massey Claim, a Red-Flags Claim, and an Information-Systems Claim each rest on the same concept: a breach of the duty of loyalty grounded on bad faith action.”).

This type of breach of loyalty became known as a *Massey* claim.¹⁶⁹ “A *Massey* claim requires an aggregation of pled facts sufficient to support an inference that a corporate fiduciary made a conscious decision to violate the law.”¹⁷⁰ Because the kinds of behavior that can sustain a *Caremark* claim can eventually cross the line to “support[] an inference that the board was consciously condoning legal conduct,” *Caremark* and *Massey* claims are often brought against directors at the same time.¹⁷¹ Like *Caremark* claims, many of the *Massey* claims that survive a motion to dismiss involve corporate harms that threatened the stability of critical infrastructure. As explained above, the *Massey* case itself involved corporate harm that claimed lives and caused property destruction but also threatened the stability of the energy sector—a critical infrastructure industry.

5. Financial Services

Stone v. Ritter – a foundational case in the *Caremark* canon - centered around harm to the financial services sector caused by a financial institution’s failure to comply with the Bank Secrecy Act’s requirements on money laundering.¹⁷² A more recent financial services case has survived the motion to dismiss stage: *Brewer v. Turner*.¹⁷³ Kathleen Brewer and her fellow shareholders sued Regions Financial Corporation’s (Regions) directors, claiming that the latter failed to sufficiently oversee and monitor compliance with financial services regulations and ignored red flags that should have alerted the directors to Regions’s long-term unlawful manipulation of overdraft fees.¹⁷⁴ The shareholders alleged that, starting in 2018, Regions’s branches systematically manipulated overdraft fees in ways that violated consumer protection laws.¹⁷⁵ The shareholders further alleged that sufficient red flags were brought to the directors attention and, in particular, in 2019 the directors had a critical opportunity to end the abusive practices and declined to do so.¹⁷⁶

The red flags, the board’s awareness of them, the decision not to act, and the continued manipulation of overdraft fees were all well documented by Regions’s former general counsel who turned whistle-blower for the Consumer Financial

¹⁶⁹ *In re Facebook, Inc. Derivative Litig.*, C.A. No. 2018-0307-JTL, Trans. at 4 (Del. Ch. May 10, 2023) (describing *Massey* claims as when there are legal violations that “support[] a pleading-stage inference that management is operating an enterprise based on recidivous law breaking”); see also Sarah Runnells Martin & Dakota B. Ecenrode, *Caremark Developments: Business Risk Versus Massey Claims*, HARV. L. SCH. FORUM ON CORP. GOV. (July 3, 2024), <https://corpgov.law.harvard.edu/2024/07/03/caremark-developments-business-risk-versus-massey-claims/#2b> (distinguishing between *Caremark* and *Massey* claims cases).

¹⁷⁰ *Ontario Provincial Council of Carpenters’ Pension Tr. Fund v. Walton et. al.*, C.A. No. 2021-0827-JTL at 75.

¹⁷¹ *Id.* at 74-75.

¹⁷² *Stone v. Ritter*, 911 A.2d at 365.

¹⁷³ C.A. No. 2023-1284-KSJM, 2025 WL 2769895 (Del. Ch. Sept. 29, 2025).

¹⁷⁴ *Id.* at *1-3.

¹⁷⁵ *Id.* at *15-16.

¹⁷⁶ *Id.* at *16-17.

Protection Bureau (CFPB).¹⁷⁷ Eventually, the CFPB issued its own investigative report and entered into a consent order with Regions that imposed penalties of \$50 million and \$141 million in payments to affected account holders.¹⁷⁸ Ultimately, the case survived dismissal as to any of the directors who served on the board at the time it was made aware of the whistle-blower complaint because the plaintiffs had adequately alleged that the board had notice of striking red flags and yet did nothing to address the concerns, to the company's detriment. A shareholder derivative action against Wells Fargo also survived dismissal when it similarly alleged a failure to establish a monitoring system to detect discriminatory lending practices.¹⁷⁹ In both cases, the alleged *Caremark* violations involved activity that threatened the stability of a critical infrastructure sector: financial services.

6. Commercial Facilities

Two recent cases involving companies in the commercial facilities sector survived motions to dismiss when the shareholder plaintiffs adequately alleged that widespread workplace harassment threatened the stability of the critical infrastructure they provided through their businesses.

First, in *In re McDonald's Corp. Stockholder Derivative Litig.*, shareholders alleged that McDonald's "Global Chief People Officer" personally harassed employees and ignored harassment by others during his four-year tenure.¹⁸⁰ Although an officer, rather than a director, the Delaware Court of Chancery determined that the officer owed a *Caremark* duty of oversight to the corporation within his area of remit because he had been entrusted by the McDonald's board with overseeing the entirety of the multi-national company's human resource division.¹⁸¹ The Court went on to conclude that the plaintiffs adequately pled a "Red-Flags Claim [that] assert[ed] that [the officer] permitted a toxic culture to develop at the Company that turned a blind eye to sexual harassment and misconduct" which ultimately led to coordinated complaints filed against the company, a thirty-city strike, a second ten-city strike, and reputational harm.¹⁸² Finally, the Court found that the plaintiffs sufficiently alleged that the officer acted in bad faith by becoming informed of the harassment, intentionally ignoring it, actively participating in it, and failing to report any of it up to the board.¹⁸³

¹⁷⁷ *Id.* at *12.

¹⁷⁸ *Id.*

¹⁷⁹ *SEB Investment Mgmt. AB, et al. v. Wells Fargo & Co., et. al.*, 22-cv-03811-TLT, Order Denying Motion to Dismiss Amended Complaint (N.D. Cal. July 29, 2024).

¹⁸⁰ *In re McDonald's Corp. Stockholder Litig.*, C.A. No. 2021-0324-JTL, at 1 (Del. Ch. Jan. 25, 2023).

¹⁸¹ *Id.* at 2-3; 26-28.

¹⁸² *Id.* at 54-56.

¹⁸³ *Id.* at 58-60.

Much has been said about whether *In re McDonald's* impermissibly expanded *Caremark* duties to encompass sexual harassment in the workplace.¹⁸⁴ But the reality is that the corporate harm alleged in *McDonald's* was not the sexual harassment. Instead, the failure to monitor and oversee compliance with anti-harassment laws threatened the stability of a company that plays a major role in the critical infrastructure sector of commercial facilities that includes retail establishments, including restaurants.¹⁸⁵ The officer's oversight failure led to a massive strike of the company's retail establishments, disrupting the commercial facilities it operated and the workforce it employed there.

The second *Caremark* case involving sexual harassment claims to survive a motion to dismiss—*Los Angeles City Employees' Retirement System v. eXp World Holdings, Inc.*¹⁸⁶—also involved corporate harm that threatened the commercial facilities sector. eXp World Holdings is a technology-forward real estate firm.¹⁸⁷ Real estate is a sub-sector of the commercial facilities sector,¹⁸⁸ and eXp World Holdings is a significant player in that sector, with operations in 24 countries, over 2,000 direct employees, and a network of over 80,000 real estate agents.¹⁸⁹

In that context, the Delaware Court of Chancery allowed the plaintiff's claims to survive the motion to dismiss when plaintiff alleged that directors violated their *Caremark* duties by consciously disregarding reports of rape, assault, and other forms of harassment of real estate agents at corporate sponsored events.¹⁹⁰ The public harm to eXp was two-fold. First, it suffered reputational damage when word of the harassment spread through social media—the very type of modern technology upon which eXp's business model rested. Second, its board's misconduct threatened the broader real estate system by making female agents feel unsafe in their workspaces.¹⁹¹ The sexual assaults enabled by the corporate culture at eXp were deplorable acts that caused private harm; the

¹⁸⁴ See, e.g., Jennifer Kay, *Delaware Split on Sexual Harassment Liability Opens New Debate*, BLOOMBERG LAW (Jan. 29, 2026), <https://news.bloomberglaw.com/litigation/delaware-split-on-sexual-harassment-liability-opens-new-debate>.

¹⁸⁵ CISA, Commercial Facilities, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/commercial-facilities-sector> (last visited Feb. 5, 2026).

¹⁸⁶ *Los Angeles City Employees' Retirement System v. eXp World Holdings, Inc.*, C.A. No. 2024-0998-KSJM (Ch. Del. Jan. 16, 2026).

¹⁸⁷ *Id.* at 1.

¹⁸⁸ CISA, Commercial Facilities, *supra* note 184.

¹⁸⁹ *eXp World Holdings (EXPI) Company Profile*, FINANCECHARTS, <https://www.financecharts.com/stocks/EXPI/profile> (last accessed Feb. 5, 2026).

¹⁹⁰ *eXp World Holdings, Inc.*, *supra* note 196, at 29 (“The allegations and legal theories underlying each of the four counts are similar. Plaintiff claims that each Defendant violated that each Defendant violated his obligations under *Caremark* by ‘failing to ensure that the Company had in place reasonable reporting and information systems that would have allowed eXp’s officers and the Board to know about and prevent acts of sexual assault and misconduct, and failing to respond to and consciously disregarding the accounts of sexual assault and misconduct that were brought to the [Defendant’s] attention.’”).

¹⁹¹ *Id.* at 63-65.

board's refusal to act when confronted with those acts set in motion events that caused public harm to the corporation that implicated critical infrastructure.

The impact on infrastructure explains why some harassment cases survived dismissal while others did not. As the Court itself noted, McDonald's is one of the largest employers in the world.¹⁹² McDonald's \$140 billion in sales makes it *the* dominant player in a specific industry in the commercial facilities sector: the quick-service restaurant (QSR) industry.¹⁹³ With those sales, McDonald's holds 15% of the \$950 billion QSR industry.¹⁹⁴ This context reveals the deeper threat the mistreatment poses by the misconduct of McDonald's Global Chief People Officer.

Other workplace harassment cases did not move forward on *Caremark* grounds because the public harm did not sufficiently threaten critical infrastructure even if there were private harms. This explains why the workplace discrimination claims against Wells Fargo were dismissed.¹⁹⁵ Wells Fargo employs 217,000 people¹⁹⁶ in comparison to McDonald's employment of roughly 2.2 million people.¹⁹⁷ Other *Caremark* cases involving workplace harassment allegations were dismissed under similar circumstances. *Brola v. Lundgren* involved claims that a director's sexual harassment of two employees constituted a per se duty of loyalty violation because sexual harassment is illegal.¹⁹⁸ The claims were dismissed because "[a]dopting Brola's theory would undermine the principled distinction between interpersonal harms and fiduciary duties."¹⁹⁹ This is the Court's recognition that, although sexual harassment caused personal harm, the public harm necessary to trigger *Caremark* duties remained lacking.²⁰⁰ Credit Glory, the company at the heart of Brola's complaint, employs only 80 people²⁰¹ and is not part of the commercial facilities sector like McDonald's and eXp Holdings, and, unlike Wells Fargo, offers only credit report dispute services rather than core access to financial services.²⁰²

¹⁹² *In re McDonald's Corp. Stockholder Litig.*, C.A. No. 2021-0324-JTL, at 1.

¹⁹³ *McDonald's Market Share: The Definitive 2026 Guide*, FLAVOR365 (Jan. 11, 2026), <https://eathealthy365.com/mcdonalds-market-share-the-definitive-2026-guide/> (last accessed February 7, 2026).

¹⁹⁴ *Id.*

¹⁹⁵ *SEB Investment Mgmt.*, *supra* note 189.

¹⁹⁶ *Wells Fargo: Number of Employees 2012-2025*, MACROTRENDS (last visited Feb. 5, 2026), <https://www.macrotrends.net/stocks/charts/WFC/wells-fargo/number-of-employees>.

¹⁹⁷ *McDonald's Employee Count: The Full Story & Facts*, FLAVOR365 (Jan. 8, 2026) (last visited Feb. 5, 2026), <https://eathealthy365.com/mcdonalds-employee-count-the-full-story-facts/>.

¹⁹⁸ *Brola v. Lundgren*, 2024-1108-LWW, Opinion, at 1 (Del. Ch. Aug. 5, 2022).

¹⁹⁹ *Id.* at 12.

²⁰⁰ *Id.* at 10-11 (explaining that the McDonald's decision "did not create a rule that a viable breach of fiduciary duty claim arises whenever an officer engages in unlawful harassment" but rather that "[i]n McDonald's, the defendant was a senior officer charged with maintaining a safe and respectful workplace at the enterprise level").

²⁰¹ *Credit Glory Management*, ROCKETREACH, https://rocketreach.co/credit-glory-management_b47342f4fc5cd9d6 (last visited Feb. 5, 2026).

²⁰² *Brola v. Lundgren*, 2024-1108-LWW, Opinion, at 1 ("Credit Glory Inc. (the 'Company') is a private Delaware corporation that assists subscribers in disputing credit report inaccuracies.").

B. *Supply Chain Resilience as a Caremark Duty*

The discussion of the cases above highlight three important lessons for corporate management: First, more successful *Caremark* claims involve both harms to the corporation and harms to national infrastructure – food and agriculture, healthcare, transportation, energy, financial services, and commercial facilities. Corporate boards must be particularly attentive to their *Caremark* duties when their corporations supply goods and services to one or more of these infrastructure sectors. This is because a lack of oversight on their part not only affects the corporation but also the viability of these sectors.

This does not mean that all cases alleging harms to critical infrastructure survive dismissal. Instead, if directors and officers fail to implement a monitoring and oversight system to ensure compliance with laws and regulations designed to prevent threats to national infrastructure, then that failure may constitute a failure to perform the information system duties of *Caremark*. Similarly, conscious disregard of red flags that signal ongoing failure to comply with laws and regulations designed to protect critical infrastructure may constitute a red flags *Caremark* claim.

The *Caremark* cases discussed above illustrate that, in either case, if directors and officers violate their *Caremark* duties in ways that cause the type of harm to the company that can endanger critical infrastructure, those claims have historically fared better than other types of corporate harms. In contrast, there is no *Caremark* violation if the oversight failures caused only private harms,²⁰³ or the directors and officers took remedial action in response to red flags²⁰⁴ – even if the corporation is part of a critical infrastructure sector. For example, when shareholders sued directors of Solarwinds Corporation for alleged “fail[ure] to adequately oversee the risk to cybersecurity of criminal attack,”²⁰⁵ the case was dismissed because the plaintiffs did not adequately plead that the directors allowed the company to violate positive law, thereby preventing a successful *Massey* claim. There was also no *Caremark* violation because the directors had in place an information system and responded to red flags once they arose.²⁰⁶

Second, the *Caremark* duty also applies to management of corporations that supply *digital* infrastructure. While the *Caremark* cases involve threats to physical infrastructure, there is no reason why the reasoning of these cases does not apply equally to those who supply digital infrastructure. In fact, *Firemen’s Retirement*

²⁰³ See, e.g., *id.* at 1 (granting motion to dismiss where harm was purely a private harm).

²⁰⁴ See, e.g., *Construction Industry Laborers Pension Fund v. Bingle, et al*, C.A. No. 2021-0940-SG (Del. Ch. Sept. 6, 2022) (dismissing red flag *Caremark* claims against an information technology company because the directors acted to remediate the harm as soon as the red flags were brought to their attention); *Enzell v. Dinges*, 137 F.4th 291 (2025) (granting motion to dismiss *Caremark* and *Massey* claims against a mining company where directors actively attempted to remediate lack of compliance in light of red flags, even if remediation was not always successful).

²⁰⁵ *Id.* at 1.

²⁰⁶ *Id.* 3-4.

System of St. Louis on behalf of Marriott International, Inc. v. Sorenson supports the position that oversight liability could attach to a failure to monitor cybersecurity risks,²⁰⁷ which is one risk to data supply chains.²⁰⁸ The case involved corporate harm that threatened stability to commercial facilities and financial services, two important infrastructure sectors. The Court took note of the fact that “[t]he President of the United States has named cybersecurity a ‘top priority and essential to national and economic security.’”²⁰⁹ It opined that “as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them.”²¹⁰ The Court explained that “[t]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.”²¹¹ Nevertheless, the Court found that an oversight system existed and that Marriott took remedial measures once the breach was discovered.²¹² As a result, whatever oversight duties the Marriott board owed with respect to cybersecurity oversight, the plaintiffs had failed to state a claim for breach of those duties.²¹³ But *Sorenson* illustrates that *Caremark* doctrine is already beginning to recognize the board’s responsibility with regard to data supply chains.

Third, corporate boards cannot fulfil their *Caremark* duties regarding infrastructure without ensuring the resilience of their supply chains. For example, the COVID-19 pandemic demonstrated that the effectiveness of the America’s health care sector depends on how well its sector participants manage their supply chains for vaccines, face masks, hand sanitizer, and medical equipment. Similarly, the effectiveness of other critical sectors, ranging from financial services to defense industrial base to energy resources—also depend on how the companies within those sectors manage their supply chain risks.

This means that board of directors within these critical sectors must not only monitor the product or service their company contributes to the marketplace—whether it is a cancer drug or commercial jet—but also their supply chains that determine whether they can sell those goods or services. Blue Bell Creameries cannot offer ice cream to the marketplace without access to dairy milk. Therefore, milk is a critical component of Blue Bell’s supply chain and it must manage its direct production or sourcing it from dairy suppliers. Similarly, Boeing has a wide range of suppliers who provide it with critical components ranging from engines to cockpits to airline seats. The failure to oversee the supply chains for these components would impede Boeing’s ability to produce aircraft for the aviation industry—thereby compromising the nation’s

²⁰⁷ *Marriott International, Inc. v. Sorenson*, C.A. No. 2019-0965-LWW, 2021 WL 4593777, at *11-*12 (Del. Ch. Oct. 5, 2021).

²⁰⁸ Kish Parella & Carla L. Reyes, *Global Supply Chain Resiliency in Emerging Technologies: A Case Study of Bitcoin Mining*, __ SEATTLE U. L. REV. __ (forthcoming 2026).

²⁰⁹ *Marriott International, Inc. v. Sorenson*, 2021 WL 4593777, at *11-12.

²¹⁰ *Id.*

²¹¹ *Id.*

²¹² *Id.* at *13.

²¹³ *Id.*

transportation sector, which is one of the critical infrastructure sectors. The strength of these sectors depends on the resilience of the supply chains maintained by that sector's member companies. As a consequence, *Caremark* duties apply to the board's management of its supply chains when it produces a product or service within the critical infrastructure sectors.

V. OPERATIONALIZING *CAREMARK*: A FRAMEWORK FOR SUPPLY CHAIN OVERSIGHT

Maintaining the availability, security and integrity of critical infrastructure, including critical and emerging technologies, is both a national security and economic strategic priority. The physical infrastructure that sat at the foundation of the economic and national security advances in the twentieth century was generally built—and continues to be maintained—directly by or through heavy subsidies of public funds. In contrast, the digital infrastructure that supports the twenty-first century economy is largely built, maintained, and operated by private companies. Re-conceptualizing *Caremark* duties to align corporate governance with national security imperatives means that corporate boards must oversee the supply chain resilience of the critical infrastructure that they support. Part A offers a framework that equips corporate boards with the tools they need to fulfill those oversight duties in good faith. Part B applies this framework to the case of Bitcoin mining, thereby demonstrating how corporate management should ensure the resilience of their supply chains that support digital infrastructure.

A. Introducing the Framework: Mapping Supply Chains, Identifying Risks, and Distinguishing Tiers

Corporate directors and officers of companies in critical and emerging technology industries should oversee the supply chain resilience for these technologies. This oversight would require that corporate directors and officers take the following steps.

First, many critical and emerging technologies are hybrid technologies that involve both an *analog supply chain* and a *data supply chain*. This means that they involve a unique combination of physical technical components and intangible software components.²¹⁴ These hybrid technologies are socio-technical systems:²¹⁵ many technical aspects of the system are vulnerable to both analog

²¹⁴ DLT requires both hardware and the DLT protocol (software). Quantum computing requires specialized software, specialized programming languages, and specially trained software developers. AI requires both powerful hardware and a nearly endless supply of high-quality data.

²¹⁵ All technologies are social technologies—they are used in a specific social context. As a result, the term socio-technical system recognizes “a recursive (not simultaneous) shaping of abstract social constructs and a technical infrastructure that includes technology’s materiality and people’s localized responses to it.” Paul M. Leonardi, *Materiality, Sociomateriality, and Socio-*

(physical) supply chain risks and data (software) supply chain risks. The social demands placed on the technical system are different in each arena of critical and emerging technology with the result that the data supply chain risks faced in each arena of C&ET take different forms. Corporate directors and officers must recognize that they have two supply chains to oversee – analog and data – and should ensure the resilience of both.

Second, each of these supply chains is vulnerable to different types of risks, such as *environmental risk*, *reputational risk*, *operational risks*, *economic risk*, and *geopolitical risks*. *Environmental risks* include the risks of natural disasters such as hurricanes, earthquakes, tornados and tsunamis that can disrupt or destroy the operation of the supply chain. In contrast, *economic risk* refers to unfavorable economic conditions that may place pressure on the supply chain. *Geopolitical conflict* can involve armed conflict between countries, threats from non-state actors, and trade wars with changes in tariff regimes and regulations. *Operational risk* is “the risk of loss as a result of ineffective or failed internal processes, people, systems, or external events that can disrupt the flow of business operations.”²¹⁶ Finally, *reputational risk* can arise from conditions in the company’s supply chain and cause damage to the company’s public image. Corporate directors and officers must anticipate these risks to both of their supply chains and take steps to prevent, mitigate and address these risks.

Third, the supply chain consists of many different suppliers that are organized in the chain. Some of these suppliers have direct contractual relationships with a company, such as Boeing. These are Boeing’s direct suppliers. But other suppliers are not in direct privity of contract with Boeing; instead, they enter into contracts with Boeing’s direct suppliers to supply the latter with critical goods and services. They are Boeing’s sub-suppliers: suppliers of its direct suppliers. Both direct suppliers and sub-suppliers can pose supply chain risks to Boeing. For example, Boeing suffers from a *direct risk* if one of its direct suppliers does not produce an engine for its jet. But Boeing suffers a multi-tier risk if it one of its sub-suppliers fails to produce a component for its direct supplier. For example, Boeing’s direct supplier of engines may rely on a sub-supplier to provide it with key components. Its failure to do so means that the direct supplier cannot produce the engine and, as a result, Boeing may not be able to produce the jet. The sub-supplier is not a direct supplier in the supply chain but is instead deeper within its network but it still poses an upstream risk to Boeing. Corporate directors and officers must pay attention to both these *multi-tier risks* and the *direct risks* in the supply chain.

Technical Systems: What Do These Terms Mean? How are They Different? Do we Need Them?, in MATERIALITY AND ORGANIZING: SOCIAL INTERACTION IN A TECHNOLOGICAL WORLD 25, 42 (Paul M. Leonardi et al. eds., 2012).

²¹⁶ Vice Vicente, *Operational Risk Management: Overview and Guide*, AUDITBOARD (Feb. 16, 2024), <https://www.auditboard.com/blog/operational-risk-management/>.

Collectively, the oversight obligation under *Caremark* requires that corporate directors and officers of companies in critical infrastructure sectors – especially those producing critical and emerging technologies – do the following:

- *Step 1: Identify both the analog and data supply chains for their goods and services*, including supply chain mapping to identify their direct suppliers and sub-suppliers
- *Step 2: Recognize the various supply chains risks* that may compromise these distinct chains – operational, regulatory, geopolitical, reputational, and environmental – and *take steps to prevent, mitigate and address them*
- *Step 3: Oversee supply chain risks created by both their direct suppliers and sub-suppliers*

B. *Applying the Framework: Bitcoin Mining Supply Chains as a Case Study*

This Article has argued that a corporate board overseeing a product or service supporting critical infrastructure has a *Caremark* duty to ensure supply chain resilience. This Part applies the framework developed above to a case study in bitcoin mining. First, the section explains why the corporate boards of bitcoin mining companies should concern themselves with supply chain resilience: the bitcoin protocol has become critical digital infrastructure and its native cryptocurrency, bitcoin, has become a national and economic security priority. As an industry related to critical digital infrastructure, directors and officers of bitcoin mining companies should carefully consider the resilience of their supply chains as part of their *Caremark* duties, including through supply chain mapping, risk identification, and identifying risk tiers.

1. Bitcoin Mining Supply Chains Matter because Bitcoin is Critical Digital Infrastructure

Information technology is one of the sixteen critical infrastructure sectors.²¹⁷ Companies operating in those sectors are required to incorporate national priorities into their risk management strategies.²¹⁸ Any technology designated as a critical and emerging technology is a national priority. Distributed ledger technology has been designated a critical and emerging technology.²¹⁹

²¹⁷ CISA, *Information Technology Sector*, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector> (last accessed Feb. 6, 2026).

²¹⁸ NSM-22, *supra* note 22.

²¹⁹ THE WHITE HOUSE, NATIONAL STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGIES, *supra* note 40, at A-1.

Blockchain protocols are one kind of distributed ledger.²²⁰ The first, and perhaps most famous, blockchain protocol is Bitcoin. Not only is the Bitcoin protocol a critical and emerging technology with national security significance, but its native cryptocurrency,²²¹ bitcoin, has also risen to prominence as a national security and economic strategic priority.²²²

The Bitcoin protocol and bitcoin cryptocurrency are national security and economic strategic priorities for slightly different reasons. Some argue that the bitcoin cryptocurrency acts as a hedge against inflation and should be kept on government balance sheets to brace against future economic turmoil.²²³ Others disagree.²²⁴ Irrespective of these differing opinions, the United States, along with at least 27 other countries,²²⁵ now hold bitcoin on their national balance sheets as a strategic reserve asset.²²⁶ Indeed, around 2.3% of bitcoin's total supply (463,000 BTC) is now owned by national governments.²²⁷ President Trump created the U.S. Strategic Bitcoin Reserve by executive order on March 6, 2025.²²⁸ The Strategic Bitcoin Reserve is funded with forfeited bitcoin seized by the government during enforcement proceedings.²²⁹ To date, the reserve

²²⁰ HILEMAN & RAUCHS, *supra* note 36, at 11. Distributed ledgers are a type of distributed database that “assume[s] the presence of malicious users (node)” and structures data processing to attempt to thwart those malicious nodes. *Id.*

²²¹ Reyes, *supra* note 35, at 1210.

²²² *Id.* at 1212.

²²³ Habib Badawi, *Crypto Reserves and Monetary Evolution: Trumpism's Bold Bet on Digital Assets*, 14 J. BUS. ECON. & FIN. 34, 40 (2025) (“Digital assets might serve as effective inflation hedges in an era of unprecedented monetary expansion by central banks worldwide.”); John Taskinsoy, *Bitcoin: A New Digital Gold Standard in the 21st Century?*, at 17 (Oct. 28, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3941857 (unpublished manuscript) (“Notwithstanding some inherent weaknesses, Bitcoin has a great potential to become a digital gold standard that the future needs.”).

²²⁴ David Krause, *The Strategic Bitcoin Reserve: A Hedge Against Inflation or Digital Mirage?*, at 1 (Mar. 2025) (unpublished manuscript) (“While proponents claim Bitcoin’s fixed supply makes it an ideal hedge against inflation, this analysis challenges that assumption by assessing its extreme volatility, shifting correlations and speculative price behavior.”), https://www.researchgate.net/publication/389818975_The_Strategic_Bitcoin_Reserve_A_Hedge_Against_Inflation_or_Digital_Mirage.

²²⁵ *Bitcoin Ownership by Country 2026*, WORLD POPULATION REV., <https://worldpopulationreview.com/country-rankings/bitcoin-ownership-by-country> (last accessed Feb. 6, 2026).

²²⁶ Bradley Peak, *Which Countries Secretly Own the Most Bitcoin—Beyond the US and China*, COINTELEGRAPH (Aug. 1, 2025), <https://cointelegraph.com/explained/which-countries-secretly-own-the-most-bitcoin-beyond-the-us-and-china>.

²²⁷ *Id.* (“While that might sound like a small percentage, it equates to tens of billions of dollars in sovereign Bitcoin wealth, giving Bitcoin a growing role in national asset strategies and state-level accumulation.”)

²²⁸ EXECUTIVE ORDER, ESTABLISHMENT OF THE STRATEGIC BITCOIN RESERVE AND UNITED STATES DIGITAL ASSET STOCKPILE (Mar. 6, 2025), <https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/>.

²²⁹ *Id.*

holds approximately 198,000 bitcoin,²³⁰ making the U.S. the largest government bitcoin holder in the world.²³¹

State governments have also moved to create bitcoin reserves: at least three states—Texas, New Hampshire, and Arizona—have enacted laws permitting the creation of a state bitcoin reserve.²³² Other states are actively considering legislation to follow suit.²³³ Texas purchased \$5 million worth of bitcoin exposure through a bitcoin ETF.²³⁴ New Hampshire issued a bitcoin-backed municipal bond.²³⁵ By elevating bitcoin to a strategic reserve asset at both the national and state levels, policymakers have declared bitcoin a national and economic security priority.

The Bitcoin protocol and other distributed ledgers also now bear the weight of being designated a national security priority. Bitcoin the cryptocurrency does not exist or hold value without the Bitcoin protocol.²³⁶ The Bitcoin protocol's purpose is to group bitcoin transactions together into blocks of data and enable networked computers operated by people and entities that do not necessarily know or trust each other to come to an agreement about the validity of transactions in bitcoin.²³⁷ They reach this agreement through a computational heavy process that strings bitcoin transactions together “in a literal chain of blocks by linking blocks of validated transactions together using one-way cryptographic hashes.”²³⁸ This validation process makes the Bitcoin protocol exceedingly tamperproof—altering data in earlier blocks will cause the hashes between blocks to be rendered invalid.²³⁹

That very tamper resistance that makes bitcoin work also makes the Bitcoin protocol interesting to policymakers as a potentially foundational technology for

²³⁰ Kelvin Munene, *Under Trump, U.S. Tops Bitcoin Reserves Among Governments with Over 198,000 BTC*, COINCENTRAL (Sept. 19, 2025), <https://coincentral.com/u-s-tops-bitcoin-reserves-among-governments-with-over-198000-btc/>

²³¹ *Id.*

²³² Trevor Laurence Jockims, *Led by Texas, New Hampshire, U.S. States Race to Prove They Can Put Bitcoin on Balance Sheet*, CNBC (Jan. 17, 2026), <https://www.cnbc.com/2026/01/17/texas-us-states-budgets-bitcoin-crypto-strategic-reserve.html?msocid=0d19d6d44ac667911bc7c5a74b3766d4>

²³³ *Id.*

²³⁴ Brian Quarmby, *Texas Buys the Bitcoin Dip, Acquiring \$5M of BlackRock's IBIT*, COINTELEGRAPH (Nov. 25, 2025), <https://cointelegraph.com/news/texas-snaps-5m-blackrock-bitcoin-etf-amid-btc-dip>.

²³⁵ Micah Zimmerman, *New Hampshire Approves First-Ever \$100 Million Bitcoin-Backed Municipal Bond*, BITCOIN MAG. (Nov. 19, 2025), <https://bitcoinmagazine.com/markets/new-hampshire-first-bitcoin-bond>

²³⁶ ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* 51-55 (2016).

²³⁷ *Id.* at 50-55.

²³⁸ Reyes & Cutler, *supra* note 51.

²³⁹ NARAYANAN, *supra* note 235.

use in modernizing the U.S. financial system and capital markets.²⁴⁰ At the end of 2025, for example, the SEC approved a proposal from DTCC to use blockchain technology to tokenize traditional U.S. securities.²⁴¹ Nasdaq is seeking clearance of its own proposal for tokenized securities,²⁴² and the SEC released new guidance on the topic.²⁴³ Collectively, these actions increasingly integrate bitcoin and blockchain technology more deeply into U.S. capital markets and signal that bitcoin, the Bitcoin protocol, and distributed ledger technology are digital infrastructure²⁴⁴ with national security and economic strategic significance.

2. Mapping Bitcoin Mining Supply Chains, Identifying Risks, and Distinguishing Tiers.

Step 1 – Map the Analog and Data Supply Chains. Bitcoin mining companies have both analog and data supply chains. The machines used to “mine” for bitcoins – rigs – need particular types of both hardware and software to function. The analog supply chain consists of mining manufacturers who produce the rigs that bitcoin mining companies use to mine for bitcoin. The rigs themselves use a specialized microchip – Application-Specific Integrated Circuit (ASIC) – that is designed to accomplish a particular task with efficiency: “calculating SHA-256 hashes, a core component of the cryptographic algorithm that ensures the Bitcoin network’s security and functionality.”²⁴⁵ There is a limited number of miner manufacturers. Bitmain dominates the market with an 82% market share, followed by MicroBT and Canaan.²⁴⁶

While these three companies may supply mining rigs, they may not supply two other components that are needed for bitcoin mining: (a) ASIC chips and (b) firmware. Bitmain, MicroBT, Canaan and other rig manufacturers incorporate advanced ASIC chips into the mining rigs that they sell to bitcoin mining companies.²⁴⁷ But they only design the ASIC chips; they do not

²⁴⁰ Hassan Shittu, *New CFTC Chair Declares “Golden Age,” Launches Future-Proof Drive to Rewrite Crypto Rules*, YAHOO FINANCE! (Jan. 20, 2026).

²⁴¹ Kevin Munene, *SEC Approval Opens Door for DTCC to Tokenize U.S. Securities Using Blockchain*, COINCENTRAL (Dec. 12, 2025), <https://coincentral.com/sec-approval-opens-door-for-dtcc-to-tokenize-u-s-securities-using-blockchain/>

²⁴² Anirban Sen, *Nasdaq Makes Push to Launch Trading of Tokenized Securities*, REUTERS (Sept. 8, 2025), <https://www.reuters.com/business/finance/nasdaq-makes-push-launch-trading-tokenized-securities-2025-09-08/>.

²⁴³ U.S. Securities & Exchange Commission, *Statement on Tokenized Securities* (Jan. 28, 2026), <https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities>

²⁴⁴ See Reyes & Cutler, *supra* note 51.

²⁴⁵ ALEXANDER NEUMUELLER, GINA C. PIETERS, KAMAR MOHADDES, VALENTIN ROUSSEAU & BRYAN ZHENG ZHANG, CAMBRIDGE DIGITAL MINING INDUSTRY REPORT: GLOBAL OPERATIONS, SENTIMENT, AND ENERGY USE 9 (2025) <https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf>.

²⁴⁶ *Id.*

²⁴⁷ *Id.*

manufacture them.²⁴⁸ They are “fabless” companies that do not own the production facilities to manufacture advanced chip wafers.²⁴⁹ Instead, they contract with companies known as “foundries” to produce the chips.²⁵⁰ The chip manufacturing market is dominated by two companies: Taiwan Semiconductor Manufacturing Company (TSMC) and Samsung Electronics.²⁵¹ The analog supply chain includes two segments that both involve a small number of market players: ASIC manufacturers (Bitmain, MicroBT, Canaan, and others) and chip manufacturers (TSMC and Samsung).²⁵²

Additionally, firmware is “the specialised software that controls and optimises the operation of mining hardware, particularly ASICs.”²⁵³ It is important because it “dictates how effectively an ASIC utilises its computational power to calculate SHA-256 hashes, the core cryptographic function that underpins Bitcoin’s security.”²⁵⁴ Miners may opt to use the firmware that comes pre-installed with mining rigs or they may contract with third parties for customized firmware.

There are also component manufacturers who produce hardware components essential for operation, such as power supplies. But the ASIC manufacturers – Bitmain, MicroBT, and Canaan, among others – generally undertake final assembly of all the components.²⁵⁵

Bitcoin miners validate the records produced by the Bitcoin protocol software. The data supply chains of Bitcoin miners therefore include the Bitcoin protocol itself, along with the pools of broadcast transactions, and any specialized software the miners use to make their mining operations more efficient and

²⁴⁸ Nico Smid, *TSMC and Samsung Dominate ASIC Supply Chains*, THE BITCOIN MINING BLOCK POST (Jan. 28, 2025), https://digitalminingsolutions.tech/tsmc-and-samsung-dominate-asic-supply-chains/?utm_source=chatgpt.com.

²⁴⁹ *Id.*; see also Colin Harper, *Bitmain Reveals The Antminer S23, The Most Powerful Bitcoin Miner Ever*, FORBES (May 31, 2025) (“Bitmain’s Antminer computers utilize TSMC’s cutting-edge ASIC chips. These ASICs are manufactured in Taiwan, but Bitmain assembles the Antminers in other countries, primarily Malaysia. The bulk of ASIC miner fabrication from Bitmain and its competitors occurs in Malaysia, Thailand, and Indonesia, all of which are subject to 10% tariffs following Trump’s 90-day pause of its reciprocal tariff schedule on April 3. Should the 10% tariffs lapse and the Trump Administration institutes its original tariff policy on these countries, U.S. bitcoin miners could face 24-36% duties on ASIC miners imported from their primary manufacturing hubs. Despite bitcoin’s rise above \$100,000, mining margins are thin following the April 2024 halving, which reduced the bitcoin per block awarded to miners from 6.25 to 3.125 BTC. Now, tariffs are hiking capital expenditure costs for the hardware at the heart of bitcoin mining”).

²⁵⁰ *Id.*; see also Jamie Redman, *Report: ASIC Giant Bitmain Pre-Orders 5nm Chips Produced by TSMC’s N5 Process*, BITCOIN.COM (May 16, 2021) (reporting that Bitmain has placed chip orders with TSMC), <https://news.bitcoin.com/report-asic-giant-bitmain-pre-orders-5nm-chips-produced-by-tsmc-n5-process/>.

²⁵¹ Smid, *supra* note 247.

²⁵² CAMBRIDGE DIGITAL MINING INDUSTRY REPORT, *supra* note 256 at 53.

²⁵³ *Id.* at 54.

²⁵⁴ *Id.*

²⁵⁵ Smid, *supra* note 247.

competitive.²⁵⁶ The Bitcoin protocol software is open-source software originally produced by a pseudonym person or persons referred to as Satoshi Nakamoto.²⁵⁷ The Bitcoin software code is now maintained by a group of core developers, who vet improvement proposals and ask Bitcoin miners to adopt software updates.²⁵⁸ The open-source code maintenance process is part of the data supply chain for bitcoin because it produces code that ensures the continued stability and availability of the protocol, and thus, the stability and value of the bitcoin cryptocurrency.

As part of their work in validating the records recorded by the Bitcoin protocol, bitcoin miners perform several transaction validation functions.²⁵⁹ When a computer broadcasts a request for a transaction, a flooding algorithm sends the transaction request throughout the Bitcoin network.²⁶⁰ All nodes in the network verify that the transaction is valid: that the private key hashes to the public key, that the bitcoin has not already been sent, that the code requesting the transaction is in a white-listed form, and that the node has not already received the same transaction from the flooding algorithm.²⁶¹ The validated transactions then sit in a pool, waiting to be included in a block and confirmed as complete.²⁶² These pools of waiting transactions and the candidate blocks formed using them are part of the data supply chain for Bitcoin mining right up until the point that a block is validated and added to the chain. Until that point, the candidate blocks and the transaction pools remains at risk of manipulation.²⁶³ Lastly, Bitcoin miners often employ specially developed scripts to make their operations more efficient.²⁶⁴ Such software also forms part of a Bitcoin miners' data supply chain, as disruption to, or resulting from, that software could disrupt the end software services Bitcoin miners seek to provide: successfully adding a candidate block and winning a mining reward.

²⁵⁶ NARAYANAN, ET. AL., *supra* note 235, at 104-110.

²⁵⁷ SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (Oct. 31, 2008), <https://nakamotoinstitute.org/library/bitcoin/>.

²⁵⁸ Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer & Nelson M. Rosario, *Blockchain Development & Fiduciary Duty*, 2.2 STAN. J. BLOCKCHAIN L. & POL'Y 139, 183-84 & n.252 (2019).

²⁵⁹ NARAYANAN, ET. AL., *supra* note 235, at 52.

²⁶⁰ *Id.* at 67.

²⁶¹ *Id.*

²⁶² *Id.* at 69 ("But just as with transactions, nodes can implement different logic—they might relay blocks that aren't valid or blocks that build off an earlier point in the block chain.")

²⁶³ This is true in many blockchain protocols. Indeed, two men recently faced criminal charges for manipulating transactions in proposed Ethereum blocks before they were added to the Ethereum protocol. Indictment, United States v. Peraire-Bueno, No. 1:24-cr-00293 (S.D.N.Y. unsealed May 15, 2024); *see also* Press Release, Dep't of Justice, *Two Brothers Arrested for Attacking Ethereum Blockchain and Stealing \$25M in Cryptocurrency* (May 15, 2024), available at <https://www.justice.gov/archives/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency>

²⁶⁴ *See, e.g.*, Michael Willson, *How AI Helps in Bitcoin Mining*, BLOCKCHAIN COUNCIL (Aug. 9, 2025), <https://www.blockchain-council.org/bitcoin/bitcoin-mining-using-ai-tools/>.

Step 2 – Identify Risks in Each Supply Chain. Each of these supply chains – analog and data – are vulnerable to supply chain risks, including *operational*, *regulatory*, and *geopolitical*.

Operational risks are “[u]nacceptable differences between actual and expected operational performance.”²⁶⁵ In the analog supply chain, one significant source of operational risk is the high market concentration for critical products or components. There is a very small number of companies that produce the mining hardware needed for bitcoin mining. But these companies do not manufacture the chips needed for mining rigs to operate. They are dependent on foundries to manufacture the chips that they design. The global foundry market is also highly concentrated with a few large companies.²⁶⁶ This market concentration can lead to the real risk that there is a shortage of mining equipment available to serve the market of bitcoin mining companies – the ones who mine for bitcoin.

Riot Platforms, a bitcoin mining company, acknowledges this risk to its investors in its Form 10-K by stating the risks of a highly concentrated market of hardware manufacturers.²⁶⁷ The lack of access to new hardware mining equipment is a problem because the increased demand for Bitcoin results in more and more mining companies racing against each other for a depleting number of Bitcoins available for mining.²⁶⁸ A bitcoin mining company’s chances of successfully mining Bitcoin relates to the ratio between its individual hashrate and the network hashrate.²⁶⁹ As more mining companies compete for bitcoins,

²⁶⁵ COSO & WBSCD, ENTERPRISE RISK MANAGEMENT: APPLYING ENTERPRISE RISK MANAGEMENT TO ENVIRONMENTAL, SOCIAL AND GOVERNANCE-RELATED RISKS 56 (Oct. 2018); see also Vice Vicente, *Operational Risk Management: Overview and Guide*, Auditboard (Feb. 16, 2024), <https://www.auditboard.com/blog/operational-risk-management/> (defining operational risk as “the risk of loss as a result of ineffective or failed internal processes, people, systems, or external events that can disrupt the flow of business operations.”).

²⁶⁶ Smid, *supra* note 247.

²⁶⁷ Riot Platforms, Inc., Annual Report (Form 10-K) at 15 (Feb. 23, 2023), <https://www.sec.gov/ixviewer/documents/20230223/riot-10k.htm> (“We plan to grow our hash rate by acquiring newer, more effective and energy-efficient miners. These new miners are highly specialized servers that are very difficult to produce at scale. As a result, there are limited producers capable of producing large numbers of sufficiently effective miners, and, as demand for new miners has increased in response to increased Bitcoin prices, we have observed the price of these new miners has increased. If we are unable to acquire enough new miners or access sufficient capital to fund our acquisitions, our results of operations and financial condition could be adversely affected, as could investments in our securities.”).

²⁶⁸ Core Scientific, Form 10-K (2024) (“In order for us to maintain its competitive position under such circumstances, we must increase our total hash rate by acquiring and deploying more mining machines, including new miners with higher hash rates. There are currently only a few companies capable of producing a sufficient number of machines with adequate quality to address the increased demand. If we are not able to acquire and deploy additional miners on a timely basis, our proportion of the overall network hash rate will decrease and we will have a lower chance of solving new blocks which will have an adverse effect on our business and results of operations.”).

²⁶⁹ Riot, Form 10-K, *supra* note 266, at 20.

the network hashrate goes up.²⁷⁰ Bitcoin mining companies face the challenge of continually upgrading their hardware – their rigs – in order to maintain a favorable ratio between their individual hashrate and the network hashrate.²⁷¹ This means that the operations of a bitcoin mining company are dependent upon a reliable supply of bitcoin mining equipment from a small group of hardware manufacturers.²⁷² This is among the reasons that contracts between bitcoin mining companies and hardware manufacture contain provisions granting options or a first right of refusal to the former for the latter's newest fleet of mining hardware.²⁷³

In the data supply chain, blockchain protocols remain vulnerable to tampering.²⁷⁴ For example, if 51% of the bitcoin miners agree to do so, they can validate illegitimate transactions and tamper with previously recorded transactions.²⁷⁵ Further, bitcoin faces significant operational risk from energy disruption because bitcoin mining is energy intensive.²⁷⁶ Bitcoin miners face high energy costs and attempt to mitigate the risk of increasing costs and energy disruptions by locating near cheap sources of power.²⁷⁷ States with traditionally low cost energy sources have seen an increase in mining operations: Washington (wind power),²⁷⁸ New York (hydropower)²⁷⁹ and Texas (self-contained grid²⁸⁰

²⁷⁰ *Id.*

²⁷¹ *Id.*

²⁷² CAMBRIDGE DIGITAL MINING INDUSTRY REPORT, *supra* note 256 at 50 (“In digital mining, the rapid development of new, more powerful and efficient hardware has spurred an arms race, among manufacturers and miners alike, where relentless innovation or the ability to deploy state-of-the-art devices dictates competitive survival.”).

²⁷³ Riot-MicroBT Master Purchase & Sale Agreement at 7 (June 24, 2023) [<https://perma.cc/M544-TV4B>].

²⁷⁴ Carla L. Reyes, *The Language Landmines of Blockchain Technology and Cryptocurrency*, in THE CAMBRIDGE HANDBOOK ON LAW AND POLICY FOR NFTs (Nizan Geslevich Packin, ed., 2024).

²⁷⁵ Michael Conklin, et. al., *Legal Recourse for Victims of Blockchain and Cyber Breach Attacks*, 23 U.C., DAVIS BUS. L.J. 135, 170 (2023)

²⁷⁶ Iqtiaar Md Siddique, et. al., *Assessing the Sustainability of Bitcoin Mining: Comparative Review of Renewable Energy Sources*, 10 J. ALT. & RENEWABLE ENERGY SOURCES 1, 2 (2024) (“Bitcoin mining machines require electrical energy to operate, and before the recent price increase, all devices in the Bitcoin network were projected to consume between 78 and 101 terawatt-hours (TWh) of electricity yearly. The network requires more power to run as the number of active machines grows.”).

²⁷⁷ *Id.* (“Because bitcoin mining is very competitive, only those miners that use the most competitive mining hardware and benefit from the lowest electricity costs or alternative energy sources will survive.”).

²⁷⁸ Kaylee Tornay, *Why Northwest Officials are Only Now Deciding How to Regulate Crypto Mining*, SPOKESMAN-REVIEW (Feb. 10, 2023), <https://www.spokesman.com/stories/2023/feb/10/why-northwest-officials-are-only-now-deciding-how/>.

²⁷⁹ Lauren Dalban, *New York Bitcoin Miners Are Buying Up Power Plants—and Communities are Fighting Back*, INSIDE CLIMATE NEWS (May 10, 2025), <https://insideclimatenews.org/news/10052025/new-york-bitcoin-mines-buying-up-power-plants/>.

²⁸⁰ Brandon Mulder, *Bitcoin Miners Flocking to Texas Want to Stabilize ERCOT's Volatile Renewables*, S&P GLOBAL COMMODITY INSIGHTS (Feb. 23, 2023, 21:55 UTC), <https://www.spglobal.com/commodity-insights/en/news-research/latest-news/energy->

with available and unused industrial infrastructure).²⁸¹ Some states even offer an incentive program for reducing power use during peak load times.²⁸² Other jurisdictions are not so friendly. In fact, some have barred bitcoin mining operations.²⁸³ Such bitcoin mining bans initially drove flocks of bitcoin miners from China to Texas.²⁸⁴ Sometimes, even in friendly jurisdictions, residents push back.²⁸⁵ Disruption of access to efficient and low cost energy poses a serious risk to the bitcoin mining data supply chain because it threatens profitability.²⁸⁶ If the power is down, the software is down and mining cannot occur no matter the sophistication of the physical mining rigs.

A *regulatory risk* is a “risk that a change in regulations or legislation will affect a security, company, or industry. . . . Regulations can increase costs of operations, introduce legal and administrative hurdles, and sometimes even restrict a company from doing business.”²⁸⁷ Bitcoin mining companies and their suppliers might increasingly confront regulatory scrutiny. Bitmain is the largest manufacturer of bitcoin mining equipment.²⁸⁸ In 2024, U.S. Customs and Border Protection stopped the import of Bitmain’s mining equipment.²⁸⁹ In

transition/022323-bitcoin-miners-flocking-to-texas-want-to-stabilize-ercots-volatile-renewables.

²⁸¹ Joel Khalili, *For Bitcoin Mines in Texas, The Honeymoon is Over*, WIRED (Mar. 6, 2024, 8:44 AM), <https://www.wired.com/story/bitcoin-mining-texas-energy-grid/>.

²⁸² See Rian Dewhurst, *How Bitcoin Mining Stabilized the Grid, Saved Texans \$18 billion, and Earned the Ire of Berkshire Hathaway Energy*, DARI (Jan. 20, 2025), <https://www.dari.org/articles/how-bitcoin-mining-saved-texans-18-billion>; Elizabeth Napolitano, *Texas Paid Bitcoin Miner More Than \$31 Million to Cut Energy Usage During Heat Wave*, CBS NEWS MONEY WATCH (Sept. 7, 2023, 3:43 PM EDT), <https://www.cbsnews.com/news/bitcoin-mining-cryptocurrency-riot-texas-power-grid/>.

²⁸³ BITCOIN POLICY INSTITUTE, POLICY BRIEF ON NEW YORK CRYPTOCURRENCY MINING: FROM MORATORIUM TO TASK FORCE (June 20, 2022), <https://www.btcpolicy.org/articles/new-york-cryptocurrency-mining-from-moratorium-to-task-force>.

²⁸⁴ Khalili, *supra* note 292; Connie Lin, *Cryptocurrency Miners are Texas-Bound. Here’s Why*, FAST COMPANY (June 16, 2021), <https://www.fastcompany.com/90647778/cryptocurrency-miners-are-texas-bound-heres-why>.

²⁸⁵ David Grossman, *New York Town Bans Bitcoin Miners*, POPULAR MECHANICS (Mar. 16, 2018 1:19 PM EDT), <https://www.popularmechanics.com/technology/infrastructure/a19456939/new-york-town-bans-bitcoin-miners/>; Keaton Peters, *Texas Leaders Worry that Bitcoin Mines Threaten to Crash the State Power Grid*, DALLAS EXAMINER (July 13, 2024), <https://dallasexaminer.com/bitcoin-mining-ercot-pollution/>; Kaylee Tornay, *Special Report: Why Northwest Officials are Deciding How to Regulate Crypto Mining*, CORVALIS ADVOCATE (Feb. 27, 2023), <https://corvallisadvocate.com/special-report-why-northwest-officials-are-deciding-how-to-regulate-crypto-mining/>.

²⁸⁶ Siddique, et al., *supra* note 275, at 2-4.

²⁸⁷ Corporate Finance Institute, *Regulatory Risk*, <https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/regulatory-risk/>

²⁸⁸ CAMBRIDGE DIGITAL MINING INDUSTRY REPORT, *supra* note 244 at 50.

²⁸⁹ Prashant Jha, *US Ports Block Chinese Bitcoin Mining Machines From Bitmain*, CCN (Nov. 26, 2024) (“The U.S. Customs and Border Protection (CBP) agency has halted shipments of Bitcoin mining machines from Chinese manufacturer Bitmain, impacting the company’s flagship

December 2024, Bitmain announced that it would begin production in the United States.²⁹⁰ But this announcement has sparked additional scrutiny. On September 2, 2025, U.S. Representative Zachary Nunn sent a letter to the chair of the Committee on Foreign Investment in the United States (CFIUS) expressing his concerns over ownership transparency of certain bitcoin mining firms and suppliers connected to China.²⁹¹ Representative Nunn wrote in his capacity as the Vice Chairman of the House Financial Services Subcommittee on National Security and the China Select Committee to convey his concerns about the expansion of digital mining operations in the United States.²⁹² He raised specific concerns about Bitmain, including “[r]eports that Bitmain is exploring direct ownership of U.S. power generation assets, which could raise long-term strategic considerations”²⁹³ and “[t]he broader policy implications of permitting foreign-manufactured Application-Specific Integrated Circuit (ASIC) machines critical to digital asset mining to enter and operate within the U.S. market.”²⁹⁴

In the data supply chain, regulatory uncertainty poses a significant risk. For example, a recent focus on whether and how to hold protocol developers, including Bitcoin protocol developers, liable for activity by users may discourage software developers from building improved code for new protocols for fear of criminal prosecution.²⁹⁵ For example, one software developer, concerned about criminal liability, sued the United States Department of Justice for declaratory judgment that building code that enabled a decentralized kickstarter was not a crime.²⁹⁶ Software developers’ fear of criminal prosecution is so great that Congress is considering enacting a law—the Blockchain Regulatory Certainty Act—to clarify that it is not a crime to write code.²⁹⁷ At the same time, however, Congress is debating a digital assets market structure bill that would expand definitions of regulated financial activity to include developers of computer code who never custody user funds.²⁹⁸ Other regulatory proposals interject similar

Antminer ASICs.”), <https://www.ccn.com/news/crypto/us-block-chinese-bitcoin-mining-machines-bitmain/>.

²⁹⁰ Curt Robson, *Bitmain Launches US Mining Line as Chinese Antminer Shipments Face Customs Scrutiny*, CCN (Dec. 20, 2024), <https://www.ccn.com/news/business/bitmain-us-mining-line-shipments-customs-scrutiny/>.

²⁹¹ Letter from U.S. Representative Zachary Nunn to Scott Bessent, Secretary of the Treasury and Chair of the Committee on Foreign Investment in the United States (CFIUS) (September 2, 2025), <https://subscriber.politicopro.com/article/2025/09/gop-lawmaker-calls-for-probe-of-chinese-bitcoin-mining-firms-00552663>.

²⁹² *Id.*

²⁹³ *Id.*

²⁹⁴ *Id.*

²⁹⁵ Molly Jane Zucerkman, *Ethereum Code Editor Resigns Over Legal Concerns for Ledger Amendment Proposal*, BITCOIN INSIDER (Feb. 15, 2018), <https://www.bitcoininsider.org/article/17743/ethereum-code-editor-resigns-over-legal-concerns-ledger-amendment-proposal>.

²⁹⁶ *Levellen v. Garland*, Complaint, No. 4:25-cv-30 (N.D. TX Jan. 15, 2025).

²⁹⁷ Press Release, Lummis, *Wyden Introduce Bipartisan Legislation to Protect Blockchain Developers from Money Transmitter Requirements* (Jan. 13, 2026),

²⁹⁸ David Zaslowsky, *The CLARITY Act Delay and What it Reveals About U.S. Crypto Regulations*, BAKER MCKENZIE BLOCKCHAIN BLOG (Jan. 16, 2026),

regulatory risk by using anti-money laundering illicit financing policy concerns to attempt to sanction activity that end users are unable to implement cybersecurity for protecting their bitcoin holdings.²⁹⁹ This regulatory uncertainty impacts the Bitcoin protocol in two ways: first, it undermines the ability of the best software developers to maintain the integrity of the Bitcoin protocol; and, second, it impacts bitcoin mining companies by preventing them from maintaining state of the art cybersecurity practices to protect the bitcoin on their balance sheet. In other words, when regulatory uncertainty causes the best Bitcoin protocol developers to fear using their expertise, the data supply chain of the Bitcoin protocol suffers increased cybersecurity risks.³⁰⁰

Finally, *geopolitical risks* arise from multiple sources including armed conflict between countries; threats from non-state actors; and trade wars with changes in tariff regimes and regulations. In the analog supply chain, one source of significant geopolitical risk is the location of many of the critical suppliers. The hardware manufacturers – Bitmain, MicroBT, and Canaan – are Chinese entities. Additionally, the foundries that supply their chips are TSMC, a Taiwanese company, and Samsung, which is South Korean. The majority of chip foundries are in Southeast Asia.³⁰¹ While Bitmain announced that it would launch production sites in the United States, it did not share its source of its chips.³⁰² If its sources are foreign, then Bitmain may continue to be subject to regulatory scrutiny – as illustrated in U.S. Representative Nunn’s letter to CFIUS. These concerns are among the reasons that a number of contracts between bitcoin mining companies and their hardware manufacturers include provisions that stipulate that all production will occur in the United States.³⁰³ Some of these contracts also allocate the regulatory risk to the suppliers who take on the duty to ensure compliance with pertinent regulations.³⁰⁴ The concentration of suppliers in China and East Asia also create an additional risk that the supply of

<https://www.lummis.senate.gov/press-releases/lummis-wyden-introduce-bipartisan-legislation-to-protect-blockchain-developers-from-money-transmitter-requirements>/<https://blockchain.bakermckenzie.com/2026/01/16/the-clarity-act-delay-and-what-it-reveals-about-u-s-crypto-regulation/>.

²⁹⁹ See, e.g., Dep’t Treas. Fin. Crimes Enforcement Network, *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions*, 31 CFR Pt. 1010 (Oct. 23, 2023), <https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions>; Doc. No. 2024-30496, *Gross Proceeds Reporting by Brokers that Regularly Provide Services Effectuating Digital Asset Sales* ¶ (a)(21)(iii)(B) (Dec. 27, 2024) (Final Rule).

³⁰⁰ Jacquelyn Melinek, *The U.S. is Losing Crypto Talent as Blockchain Devs Seek Safer Havens*, TECHCRUNCH (Apr. 5, 2023), <https://techcrunch.com/2023/04/05/the-us-is-losing-crypto-talent-as-blockchain-devs-look-for-safer-havens/>.

³⁰¹ Smid, *supra* note 247 (reporting that approximately 80% of the foundry market share is in Taiwan or South Korea).

³⁰² James Morales, *Chinese Mining Giant Bitmain To Launch US HQ, Start Production in 2026*, CCN (July 29, 2029).

³⁰³ Riot-MicroBT Master Purchase & Sale Agreement at 2 (June 24, 2023)[<https://perma.cc/M544-TV4B>].

³⁰⁴ *Id.*

critical components – such as semiconductor chips – and the finished products, the mining rigs, will be curtailed if there is armed conflict in the region.

The threat of conflict also endangers logistical support. For example, in 2021, Bitcoin mining companies Riot, Bitfarms and Marathon Digital experienced delays in receiving their Bitcoin mining equipment because of global logistics issues.³⁰⁵

In the data supply chain, geopolitical risks stem from cyber-tactics that might destabilize the bitcoin protocol. For example, if a single actor or group of actors control over 50% of the hash rate, they can manipulate the Bitcoin blockchain. The rapid rise of national strategic bitcoin reserves may give governments a reason to pay closer attention to, and even interfere with Bitcoin mining in an attempt to control more hash rate.³⁰⁶ A more extreme version of geopolitical fights for protocol control might arise if governments decide to mine bitcoin themselves. If governments engage in the mining process directly, they may capture an opportunity to launch a 51% attack directly. More likely, governments will simply target multinational mining companies or mining pools within their jurisdiction as a way to disrupt the hash rate balance or achieve a competitive advantage over other countries. Ultimately, bitcoin mining manipulation might become a tool in cyber-based geopolitical maneuvering.

Step 3 – Distinguish Supply Chain Risks in Different Tiers. In a supply chain, a bitcoin mining company contracts with a group of suppliers, its direct suppliers. For example, Riot is a Bitcoin mining company but it contracts with mining hardware manufacturers - Bitmain, and MicroBT – for its mining equipment. But these manufacturers have their own suppliers because, as discussed above, they do not manufacture their own ASIC chips that are needed for the mining rigs that they sell to Riot. They likely contract with TSMC or Samsung to fabricate the chips that they design. The result is that Riot's supply chain has both direct suppliers (Bitmain, MicroBT) and also sub-suppliers (TSMC, Samsung). Each of these suppliers can be a source of risk for Riot and other bitcoin mining companies.

They confront *direct* risks from their direct suppliers with whom they are in a contractual relationship. Direct risks relate to supply chain interruptions between Riot, or another bitcoin mining company, and its manufacturers, Bitmain or MicroBT. But Riot and other bitcoin mining companies confront *multi-tier* risks from their sub-suppliers because these risks arise from the contractual arrangements between the hardware manufacturer and the chip

³⁰⁵ Wolfie Zhao, *The Global Supply Chain Crisis is Disrupting Shipments to U.S. Bitcoin Mining Firms*, THE BLOCK (Nov. 3, 2021, at 11:33 AM EDT), <https://www.theblock.co/post/123133/supply-chain-crisis-bitcoin-mining-shipments>

³⁰⁶ Indeed, Bhutan, which holds 11,286 BTC worth \$1.3 billion as of this writing, is apparently engaged in government-sponsored bitcoin mining. Eddie Mitchell, *Top Government Bitcoin Holders: Global Portfolio's Steady as Bitcoin Retreats to \$115,000*, CCN (Aug. 1, 2025), <https://www.ccn.com/news/crypto/bhutan-top-crypto-nations-full-list-of-countries/>.

foundry. For example, if the foundry cannot supply chips, then the hardware manufacturer cannot supply rigs. But the bitcoin mining companies are not in privity of contract with their sub-suppliers because they do not have a direct contractual relationship with them. But they are exposed to any risks that might originate in that tier of the supply chain even if they are not party to those contracts. This is why Riot discloses to its investors in its Form 10-K: “[T]he ongoing global supply chain crisis, coupled with increased demand for computer chips, has created a shortfall of semiconductors, resulting in challenges for the supply chain and production of the miners we employ in our Bitcoin Mining operations.”³⁰⁷

In the data supply chain, identifying direct risks and distinguishing them from multi-tier risks requires assessing the various systems at work in maintaining the Bitcoin protocol software. Direct risks in the Bitcoin protocol’s data supply chain stem from disruptions in transaction flows between bitcoin miners. Multi-tier risks stem from the layered components and social contexts that affect the systems that maintain the Bitcoin protocol. For example, the Bitcoin protocol’s decentralized structure expands the nature, scope and risks to the Bitcoin mining data supply chain. Thus, multi-tier risks include disruptions in developers’ work on maintaining the integrity of the Bitcoin protocol, disruptions in energy supply, and risky behavior undertaken by end users.

Identifying data supply chain risks—whether direct or multi-tier—requires some level of technical expertise and a deep understanding of how Bitcoin miners interact with the Bitcoin protocol (direct risks) and Bitcoin protocol governance more broadly (multi-tier risks). Bitcoin mining companies only address direct risks by keeping the software the mining rigs use up-to-date and protecting it from vulnerabilities. To properly ensure resiliency of the Bitcoin protocol, bitcoin miners must also be attuned to protocol governance proposals from the core developers, potential policy changes affecting energy availability and cost, and moves by end users to consolidate bitcoin holdings—including through strategic bitcoin reserves. Managing resiliency in the face of these multi-tier risks takes on heightened importance as investment in bitcoin by world governments places the burden of sovereign wealth and national security squarely on the shoulders of bitcoin and Bitcoin miners.

CONCLUSION

Corporate boardrooms have become sites of national security policymaking. It is corporate directors, officers and other industry actors who make the day-to-day decisions that determine the strength or weakness of the nation’s critical infrastructure. This reality raises the stakes of corporate decision-making: a failure of corporate governance presents a national security risk. These risks only grow as geopolitical conflict intensifies around the world.

³⁰⁷ Riot, Form 10-K, *supra* note 266, at 16.

Policymakers have established priorities, strategies, and objectives to ensure national security but, as in the case of critical infrastructure, they cannot implement successfully without the cooperation of the private sector. This sector responds to incentives created by the marketplace and may, therefore, underinvest in the resiliency capabilities necessary to achieve national security goals.

The misalignment between public policy and corporate priorities presents an ongoing challenge. Regulation is often treated as a tool to align interests that may otherwise diverge. Policymakers resort to both sticks and carrots to nudge corporate behavior along preferred paths, including direct equity investments. But additional regulatory regimes may be unnecessary if corporate law can fix this divergence through fiduciary duties. The duty of oversight already serves both public and private functions. It requires that directors and officers remain informed about risks to the corporation, thereby enabling them to act on that information to protect the corporation. But it is triggered in situations when failed oversight creates public risks in addition to private ones. As a consequence, the duty of oversight guards against both risks to the corporation (such as financial losses) and risks to the nation (threats to critical infrastructure). The *Caremark* duty supplies a governance mechanism that aligns public interest with private incentives. Its application demonstrates the importance of corporate law to achieving national security objectives. As such, policymakers should recognize corporate law as a potentially critical component of national security governance.

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities*.

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

ECGI Working Paper Series in Law

Editorial Board

Editor	Amir Licht, Professor of Law, Harry Radzyner Law School, Reichman University
Consulting Editors	Hse-Yu Iris Chiu, Professor of Corporate Law and Financial Regulation, University College London Martin Gelter, Professor of Law, Fordham University School of Law Geneviève Helleringer, Professor of Law, ESSEC Business School and Oxford Law Faculty Kathryn Judge, Professor of Law, Columbia Law School Wolf-Georg Ringe, Professor of Law & Finance, University of Hamburg
Editorial Assistant	Asif Malik, ECGI Working Paper Series Manager

<https://ecgi.global/content/working-papers>

Electronic Access to the Working Paper Series

The full set of ECGI working papers can be accessed through the Institute's Web-site (<https://ecgi.global/content/working-papers>) or SSRN:

Finance Paper Series	http://www.ssrn.com/link/ECGI-Fin.html
Law Paper Series	http://www.ssrn.com/link/ECGI-Law.html

<https://ecgi.global/content/working-papers>