FORTHCOMING — Journal of Critical Infrastructure Policy

Interdisciplinary Analytics in Supply Chain Trust Frameworks: Toward a Unified Model for Public-Private Intelligence Governance

Dr. Maria Gonzalez

Deputy Director for Policy, PLIANT Institute | m.gonzalez@projectpliant.com

Accepted: March 2026 | Expected Publication: Q3 2026 | PLIANT-WP-2026-03

Abstract

The governance of intelligence sharing between public agencies and private sector logistics operators presents a fundamental institutional design challenge: how to enable the information flows necessary for collective security without creating accountability gaps, competitive distortions, or legal liabilities that undermine participation. This paper develops a unified analytical framework for supply chain intelligence governance, drawing on institutional economics, regulatory theory, and case analysis of existing public-private intelligence sharing arrangements in the United States, European Union, and Australia. We identify the conditions under which voluntary sharing frameworks succeed and fail, propose a set of design principles for mandatory disclosure regimes, and discuss the implications for allied coordination on critical infrastructure intelligence governance.

Keywords: *supply chain intelligence, public-private partnerships, information governance, mandatory disclosure, critical infrastructure, institutional design*

1. Introduction

The security of global supply chains depends in significant measure on the quality of intelligence available to the actors responsible for protecting them. Governments possess classified threat intelligence that private logistics operators lack; private operators possess operational intelligence about their own networks, vulnerabilities, and incident histories that government agencies cannot easily obtain. The theoretical case for sharing across this boundary is straightforward — both parties would be better off with access to each other's information — but the institutional reality is considerably more complex.

Voluntary sharing frameworks have proliferated in the United States and allied countries over the past two decades, driven by post-9/11 recognition that critical infrastructure security requires public-private collaboration. The results have been mixed. Some frameworks — particularly those in the financial sector — have achieved genuine intelligence sharing at scale. Others have produced largely ceremonial participation with limited operational impact. Understanding what drives this variation is both academically important and practically urgent as policymakers consider expanding mandatory disclosure requirements to the logistics sector.

This paper makes three contributions. First, it develops a theoretical framework for analyzing the governance of supply chain intelligence sharing, grounded in institutional economics and regulatory theory. Second, it applies that framework to a comparative case analysis of existing sharing arrangements. Third, it derives a set of design principles for mandatory disclosure regimes that are grounded in the empirical record of what has and has not

worked in voluntary contexts.

2. Theoretical Background

The governance of intelligence sharing presents a classic collective action problem. Each participating organization bears the costs of sharing — disclosure of sensitive operational information, legal exposure, competitive risk — while the benefits of improved collective security are distributed across all participants regardless of individual contribution. This structure creates incentives for free-riding: organizations that consume shared intelligence without contributing their own, and organizations that participate nominally while withholding the most sensitive and valuable information.

The institutional economics literature identifies several mechanisms for overcoming collective action problems in information sharing contexts. Ostrom's work on common pool resource governance identifies the importance of clearly defined membership, graduated sanctions for non-compliance, and low-cost conflict resolution mechanisms. Ayres and Braithwaite's responsive regulation framework emphasizes the value of starting with voluntary compliance mechanisms and escalating to mandatory requirements only where voluntary mechanisms demonstrably fail. Both frameworks have influenced the design of existing public-private intelligence sharing arrangements, with varying degrees of fidelity.

2.1 The Trust Problem

A distinctive feature of supply chain intelligence sharing — compared to financial sector information sharing, which has received more analytical attention — is the asymmetric trust structure between participants. In financial sector sharing arrangements, participating institutions are broadly comparable in size, regulatory exposure, and legal sophistication. In supply chain sharing arrangements, government agencies, large multinational logistics operators, and small terminal operators participate in the same frameworks despite vastly different institutional capacities, legal resources, and risk tolerances.

This asymmetry creates what we term the trust differential problem: smaller operators are asked to share sensitive operational information with government agencies and large competitors in frameworks where they have limited ability to verify how that information will be used, stored, or protected. The rational response to this uncertainty — minimal, nominal participation — is precisely what undermines the collective value of sharing arrangements.

3. Comparative Case Analysis

We analyze three existing public-private intelligence sharing arrangements with relevance to supply chain security: the U.S. Maritime Cyber Readiness Branch information sharing program, the EU NIS2 Directive incident reporting framework, and Australia's Critical Infrastructure Risk Management Program. Each case is assessed against five governance dimensions: participation breadth, information quality, enforcement architecture, accountability mechanisms, and allied interoperability.

3.1 U.S. Maritime Cyber Readiness Branch

The Maritime Cyber Readiness Branch (MCRB), established within the U.S. Coast Guard Cyber Command, operates a voluntary information sharing program for maritime infrastructure operators covering cyber incident reporting, threat intelligence distribution, and vulnerability disclosure. Participation has grown steadily since the program's 2018 launch, with approximately 340 registered participants as of 2024.

Participation breadth is moderate — the program reaches large terminal operators and major shipping lines effectively but has limited penetration among smaller operators and feeder service providers that collectively account for significant throughput at secondary nodes. Information quality is assessed as high among active participants but variable overall, reflecting the voluntary nature of incident reporting.

3.2 EU NIS2 Directive Framework

The NIS2 Directive, which entered into force across EU member states in October 2024, establishes mandatory incident reporting obligations for operators of essential services including maritime transport, port operations, and logistics. The directive represents the most significant expansion of mandatory disclosure requirements for logistics sector operators among G7 jurisdictions and provides a useful model for assessing the operational implications of mandatory versus voluntary frameworks.

Early implementation data suggests that mandatory reporting requirements have substantially increased incident disclosure rates among previously non-participating operators, but that information quality has been uneven — mandatory reports tend to be more formulaic and less operationally detailed than voluntary submissions from engaged participants. This quality-quantity tradeoff is a persistent feature of mandatory disclosure regimes across sectors.

3.3 Australia's Critical Infrastructure Risk Management Program

Australia's Security of Critical Infrastructure Act, significantly amended in 2022, establishes the most comprehensive mandatory disclosure and risk management framework among anglophone allied nations. The Act requires operators of critical infrastructure assets — including port facilities and logistics networks — to develop and maintain risk management programs, report cyber incidents within defined timeframes, and provide government with information access rights in defined circumstances.

The Australian framework is notable for its explicit allied interoperability provisions, which establish data-sharing arrangements with the United States, United Kingdom, and Canada for critical infrastructure intelligence. This interoperability architecture provides a partial model for the kind of allied coordination that is currently absent from U.S. logistics sector intelligence sharing arrangements.

4. Design Principles for Mandatory Disclosure Regimes

Drawing on the comparative case analysis and the theoretical framework developed in Section 2, we propose six design principles for mandatory disclosure regimes in the logistics sector:

> **Principle 1: Tiered Obligation Structure.** Mandatory disclosure obligations should be calibrated to operator size and strategic significance. Large operators of critical nodes should face more extensive obligations than small operators of secondary facilities. Uniform requirements impose disproportionate burdens on smaller operators while providing limited security benefit.
>
> **Principle 2: Protected Disclosure Channels.** Mandatory disclosure frameworks must provide credible legal protections for reported information — against use in civil litigation, against competitive disclosure, and against Freedom of Information Act release. Without such protections, operators will satisfy the letter of disclosure requirements while withholding operationally significant detail.
>
> **Principle 3: Reciprocal Government Disclosure.** Mandatory private sector disclosure should be paired with government commitments to share relevant threat intelligence with disclosing operators. Asymmetric

disclosure frameworks — in which government receives but does not share — systematically undermine the trust necessary for high-quality voluntary participation.

Principle 4: Independent Oversight. Mandatory disclosure frameworks should include independent oversight mechanisms with authority to assess compliance quality, not merely compliance volume. Formulaic reporting that satisfies formal requirements while providing no operational value should be identifiable and addressable.

Principle 5: Allied Interoperability. Disclosure frameworks should be designed from the outset for allied interoperability, with data standards and sharing arrangements that enable cross-border intelligence synthesis. The current patchwork of incompatible national frameworks substantially reduces the collective security value of individual national programs.

Principle 6: Graduated Enforcement. Enforcement mechanisms should follow a graduated structure — starting with remediation requirements for good-faith non-compliance and escalating to financial penalties only for deliberate or repeated violations. Aggressive early enforcement deters participation and undermines the trust-building function of disclosure frameworks.

5. Implications for Allied Coordination

The comparative analysis and design principles developed here have direct implications for allied coordination on supply chain intelligence governance. The current landscape — in which the United States, European Union, United Kingdom, Australia, and other allied nations maintain largely separate and incompatible disclosure frameworks — represents a significant collective security gap. Threat actors operating across allied jurisdictions can exploit the seams between national frameworks in ways that no single national program can detect or address.

Closing this gap requires not merely technical interoperability between national reporting systems — though that is necessary — but harmonization of disclosure obligations, protected channel architectures, and enforcement approaches sufficient to enable genuine cross-border intelligence synthesis. The Australian framework's explicit interoperability provisions provide a useful starting point, but a comprehensive allied framework would require substantially more ambitious coordination than has been achieved to date.

PLIANT is currently engaged with CISA, DHS S&T;, and allied counterpart organizations on a research program examining the feasibility of a Five Eyes supply chain intelligence sharing framework. Results from that program will inform a forthcoming policy brief addressing the institutional architecture required for allied-level coordination.

6. Conclusion

The governance of supply chain intelligence sharing is a solvable institutional design problem, but only if policymakers resist the temptation to treat it as primarily a technical problem. The barriers to effective sharing are not primarily about data formats or secure transmission protocols — they are about trust, incentives, accountability, and the credibility of government commitments to protect disclosed information and reciprocate with threat intelligence. Getting the institutional design right is a precondition for the technical architecture to deliver its potential value.

The six design principles proposed here are grounded in the comparative record of what has and has not worked in existing sharing arrangements and are intended to be practically actionable for policymakers designing or reforming disclosure frameworks. PLIANT welcomes engagement from government partners and logistics sector stakeholders on the application of these principles to specific regulatory design challenges.

Acknowledgments: The author thanks Dr. James Patterson and Dr. Michael Torres for comments on earlier drafts, and PLIANT's government partners for engagement on the comparative case analysis. Research was conducted under PLIANT internal funding. The author declares no conflicts of interest. Correspondence: m.gonzalez@projectpliant.com

---