Supply Chain Disclosure & Transparency in Critical Infrastructure

Authors: Dr. Maria Gonzalez · Dr. James Patterson

Document ID: PLIANT-J-2026-01 | PLIANT Institute, Palo Alto CA | projectpliant.com

Executive Summary

This policy brief examines the current landscape of supply chain disclosure requirements for critical infrastructure operators, identifies material gaps in existing regulatory frameworks, and proposes a tiered mandatory disclosure model designed to reduce information asymmetries without imposing disproportionate compliance burdens on private sector operators. The brief draws on PLIANT's research into procurement transparency, Atlas database findings on disclosure gap patterns, and comparative analysis of existing disclosure regimes across G7 jurisdictions.

1. The Disclosure Problem

Critical infrastructure operators in the logistics sector operate under a patchwork of disclosure requirements that vary significantly by jurisdiction, sector, and ownership structure. The result is a landscape of systematic information asymmetries that disadvantage regulators, allied governments, and legitimate commercial actors while creating opportunities for exploitation by state and non-state threat actors.

PLIANT's Atlas database documents over 340 instances in which disclosure gaps — the absence of required or reasonably expected information about sub-tier suppliers, digital infrastructure, or foreign ownership relationships — contributed to a documented disruption or security incident. In 41% of these cases, the disclosure gap reflected deliberate non-disclosure by a party with material interest in concealment.

> **The most consequential disclosure gaps are not those involving classified information — which is governed by existing frameworks — but those involving commercially sensitive operational data that falls into a regulatory grey zone between public disclosure requirements and legitimate confidentiality claims.**

2. Comparative Regulatory Landscape

A comparative analysis of G7 disclosure regimes reveals substantial variation in the scope and enforceability of supply chain transparency requirements. The United States maintains the most developed framework for defense-adjacent supply chains through DFARS and CMMC requirements, but commercial logistics operators outside the defense industrial base face significantly lighter disclosure obligations. The European Union's NIS2 Directive represents the most comprehensive recent effort to extend cybersecurity disclosure requirements to logistics operators, but implementation has been uneven across member states.

Japan, Canada, and the United Kingdom maintain intermediate frameworks that are stronger than U.S. commercial requirements but lack the enforcement mechanisms necessary to deter deliberate non-disclosure. Australia's critical infrastructure legislation, updated in 2022, represents the most aggressive recent expansion of mandatory disclosure obligations and provides a useful model for allied coordination efforts.

3. Proposed Disclosure Framework

PLIANT proposes a three-tier mandatory disclosure framework for critical infrastructure logistics operators:

Tier 1 — Public Disclosure. Ownership structure, primary sub-tier supplier relationships, and digital infrastructure categories. Applicable to all operators above a defined throughput threshold.

Tier 2 — Regulator Disclosure. Foreign ownership relationships, terminal operating system architecture, and cyber incident history. Disclosed to designated regulatory bodies under confidentiality protections.

Tier 3 — Classified Disclosure. Detailed vulnerability assessments, foreign intelligence contact history, and classified partner intelligence. Handled under existing government classification frameworks.

4. Implementation Considerations

Effective implementation requires resolution of three primary challenges: jurisdictional coordination across G7 and partner governments, confidentiality protections adequate to address legitimate commercial sensitivity concerns, and enforcement mechanisms capable of deterring deliberate non-disclosure. PLIANT is currently engaged with CISA and DHS S&T; on a pilot disclosure framework applicable to maritime terminal operators, with results expected in mid-2027.

5. Conclusion

The information asymmetries that characterize global logistics networks are not an incidental feature of market complexity but a structural condition that is actively maintained by actors with interests in opacity. Closing these gaps requires a coordinated regulatory response that matches the sophistication of the threat environment. The tiered framework proposed here represents a practical path toward greater transparency that accommodates legitimate confidentiality concerns while establishing meaningful accountability for deliberate concealment.