



WRITTEN SUBMISSION

Regulatory Approach under Bill C-35: Interoperable, Audit-Ready Evidence for Effective Forced-Labour Enforcement

Practitioner input on traceability, evidentiary integrity, interoperability, SME proportionality, and implementation supports

Submitted by: Chris Papp, Founder & CEO, TransPacific Trade Nexus (TPTN), Montréal, Québec

Operating entity: 16422411 Canada Inc. (operating as SynergAI)

Consultation: Public consultation on regulatory approach under Bill C-35, *An Act respecting the prohibition of the importation of goods produced by forced labour* (Global Affairs Canada and the Canada Border Services Agency)

Date: August 12, 2026

Scope: This submission addresses the evidentiary and implementation aspects of the proposed regulatory approach: the evidentiary architecture behind information requirements, traceability and chain of custody, interoperability, digital implementation supports, SME proportionality, information governance and selective disclosure, and the accountable use of AI-assisted systems. It does not address whether particular goods, producers, or regions should be listed; worker-remediation policy; the substantive legal test for forced labour; civil liability; or broader human-rights policy, which fall outside the contributor's area of trade-execution and digital-governance practice.

1. Purpose and Standing

This submission is provided as practitioner input on the evidentiary, traceability, and implementation aspects of the proposed regulatory approach. It reflects more than 25 years of operating experience in global trade, cross-border documentation workflows, and compliance execution. The perspective is further informed by the contributor's public-review contributions to the UN/CEFACT United Nations Transparency Protocol concerning identity resolution, selective disclosure, and evidentiary integrity;^[5] participation as a Participating Expert in the UN/CEFACT eCMR Working Group; membership on the Standards Council of Canada Canadian Mirror Committee for ISO/TC 309 (Governance of Organizations); and participation in Digital Governance Standards Institute technical committees, including Artificial Intelligence and Digital Trust and Identity. These references are provided solely to establish relevant practitioner standing and do not imply endorsement by any organization.

The submission is deliberately scoped. It does not respond to every question in the consultation paper. It concentrates on a single question the paper raises but must resolve for the regime to function in practice: what a credible electronic evidence architecture behind the import prohibition should contain, how it should behave, and how it can be implemented without imposing disproportionate burden on legitimate traders, particularly small and medium-sized enterprises. Nothing in this submission should be read as asserting an existing relationship, endorsement, or commitment on the part of any department or official. It is contributed on the merits, for the public record.

2. The Enforcement and Evidence Gap

Canada's challenge under the proposed regime is not principally the existence of a prohibition. It is the ability to obtain, attribute, verify, and audit credible evidence about where goods and their inputs came from and how they were produced. The consultation paper identifies the underlying difficulty precisely: goods produced with forced labour carry no physical characteristic that distinguishes them at the border, global supply chains are frequently complex and opaque, and the detailed production information needed to assess risk can be hard to obtain.^[4] An enforcement regime built on requesting information is only as effective as the evidentiary system that stands behind the request.

A document requirement is not yet an evidence architecture. An importer could provide a large volume of documents in response to a request and still leave a customs officer unable to answer the questions that determine whether the goods should be admissible: who supplied each assertion, whether that person was authorized to speak for the supplier, when the information was current, what was independently verified as distinct from self-declared, whether a certification expired or changed, which upstream facility relates to which material input, whether anything was amended after the shipment began, and whether the officer can reconstruct the chain without asking the importer to rebuild it by hand. Static, unstructured documentary submissions can make these questions difficult to answer consistently and efficiently, and reconstructing the answers shipment by shipment is precisely the burden the paper's proposed burden-management measures are intended to reduce.

The implementation objective this submission recommends is therefore a reusable, interoperable, and audit-ready evidentiary architecture that allows authorized parties to obtain and assess relevant supply-chain evidence across the transaction lifecycle without requiring the evidentiary record to be reconstructed for every regulatory purpose. Expressed as an organizing principle: **collect once, evidence many times**. The same underlying evidence should be capable of serving distinct legitimate purposes rather than being assembled afresh each time a shipment is questioned. The sections that follow set out the principles such an architecture should satisfy, apply them to the specific questions in the consultation, and propose how the Government could test any candidate infrastructure before relying on it at scale.

3. Principles for an Effective Evidentiary Architecture

Five principles determine whether an evidence architecture can actually support enforcement. They are stated here once and referenced, rather than repeated, in the question responses that follow.

3.1 Attributability and provenance. Evidence used to support or contest admissibility should be attributable. Where applicable, a material evidentiary element should identify its source, the party making the assertion, the organization that party represents, the authority or role under which the assertion is made, the issuer, the date, the verification status, the validity period, and any subsequent amendment or revocation. Traceability should establish not only where information came from, but who asserted it, under what authority, when it was valid, and whether it subsequently changed. Attribution is a necessary condition of a credible evidentiary record. It does not by itself establish the truth of the underlying assertion, but it enables a reviewer to assess its source, authority, status, and evidentiary weight.

3.2 Reusability and interoperability. The same underlying evidence should not have to be reconstructed separately for a C-35 information request, for obligations under the *Fighting Against Forced Labour and Child Labour in Supply Chains Act*,^[5] for a future due-diligence regime, for other authorized federal compliance purposes, or for compatible foreign regulatory requirements. Reusability requires interoperability at the data layer: common semantics and structured formats that allow evidence to be exchanged and understood across systems without loss of meaning. Reuse does not mean unrestricted government-wide disclosure; it means that structured evidence can be reused where legally authorized and purpose-appropriate.

3.3 Evidentiary continuity and version history. Evidence must survive change. Amendments, supplier substitutions, updated certifications, corrected declarations, transport and transshipment events, and transitions between paper and digital media should not erase the prior state of the record. An architecture should preserve the prior state, the amended state, the identity of who changed it, and when and why, so that an officer can reconstruct what the record showed at any relevant point. Evidence that silently overwrites itself is weak evidence.

3.4 Proportionate, purpose-bound disclosure. Enforcement effectiveness does not require wholesale publication of supplier networks, contracts, or commercially sensitive relationships. The architecture should support minimum-necessary disclosure, role-scoped access, authorized regulator access, access logging, and a clear distinction between evidence disclosed confidentially for enforcement and information disclosed publicly for accountability. Proportionate access protects legitimate commercial confidentiality and, where relevant, the safety of workers and sources, without weakening the authority's ability to see what it needs.

3.5 Accountable automation and human authority. AI-assisted systems may assist by identifying missing information, surfacing inconsistencies, comparing data across records, flagging unusual evidentiary patterns, routing cases, and preparing material for human review. They must not determine that forced labour occurred or determine the legal admissibility of goods. That determination remains with the responsible authority. Automation in this domain should be designed to support inspection and to survive audit, with consequential decisions reserved to accountable human or institutional actors.

4. Responses to Selected Consultation Questions

The following responses address the questions where the contributor has genuine standing. Each adds question-specific recommendations and refers back to the principles in Section 3 rather than restating them.

Part 1, Q3 - Relationship to existing measures. C-35 should complement Canada's existing measures by sharing an evidentiary foundation with them rather than establishing a separate, disconnected evidence silo. Underlying supply-chain evidence collected or maintained in support of one legitimate compliance process, including where applicable reporting obligations under the Supply Chains Act,^[3] should be capable of being reused where authorized and relevant in responding to a C-35 information request, and evidence assembled in relation to an import transaction should be capable of contributing to organizational reporting where appropriate. The design objective is the same underlying evidence serving different statutory purposes, per principle 3.2. This should be pursued as compatibility and reuse, not as legal equivalence: reuse of evidence must never be treated as automatic satisfaction of a distinct legal obligation, and each regime's legal test and decision authority remain its own.

Part 1, Q7 - Implementation supports. This is where the Government can most directly reduce compliance burden while improving evidentiary quality. The most useful supports are common evidence definitions; structured, machine-readable templates and reference formats; a published evidence hierarchy that distinguishes business- or supplier-declared information, independently verified or certified information, and authoritative or government-sourced information; conformance profiles or test environments against which businesses and their service providers can prepare; phased implementation; practical guidance oriented to SMEs; and compatibility with the intermediaries that already handle much of this work, including customs brokers and logistics providers. The consultation paper's own recognition that burden can be managed through interoperable digital traceability platforms, harmonized reporting templates, phased implementation, and safe-harbour mechanisms is well founded;^[4] the recommendation here is to pursue those supports on a technology-neutral basis, specifying the evidentiary and interoperability outcomes required rather than endorsing any particular platform.

Part 1, Q8 - International alignment. Canada should align at the evidence and data layer rather than by replicating another jurisdiction's reporting form. Alignment to established international reference models

such as the UN/CEFACT Buy-Ship-Pay reference data model and the World Customs Organization Data Model^[4] can support interoperability for relevant trade-actor, transaction, transport, and regulatory data, allowing evidence prepared for the Canadian regime to be understood by compatible foreign systems. Labour-specific evidence requirements would still need clearly defined schemas and provenance rules appropriate to this regime. The objective is to avoid a Canada-specific evidence silo that Canadian businesses must later remap for every export market, consistent with principle 3.2.

Part 2A, Q2 and Q3 - Evidence importers should provide, and what best supports verification. The consultation paper identifies four candidate categories of tracing information:^[5] overall supply-chain information, supplier and entity documentation, merchandise and transaction records, and production and traceability information. This submission recommends structuring these as a common evidentiary core with defined elements rather than an open-ended documentary demand. Such a core could contain: identity and relationship elements (supplier and manufacturer identity, production facility, relevant commercial relationship); goods and inputs elements (product, commodity classification, material inputs, origin and production location); transaction elements (purchase, sale, and shipment linkage, and material transport or handoff events); and labour and due-diligence evidence (applicable certifications, audits, due-diligence actions, and identified risks with mitigation where relevant). Each element should carry the provenance metadata described in principle 3.1: source, issuer, date, verification status, validity, and amendment history. This is what allows a verifier to assess the source, status, and weight of the evidence rather than receiving an undifferentiated package of documents. The provenance layer is proposed here as policy architecture for the regime to adopt.

Part 2B, Q7 - SME proportionality. Documentation requirements should be balanced against administrative burden through proportionality by design rather than through blanket relief. Canada had 163,881 goods-importing enterprises in 2023.^[6] The scale and diversity of that importer population make proportional implementation important, even though C-35 information requirements would apply only in the circumstances prescribed for listed goods. A proportional regime should distinguish a common minimum evidence core, applicable broadly, from additional requirements triggered by risk, commodity, or the fact of listing and a formal information request, and should escalate documentation depth on that basis rather than requiring maximal documentation of every transaction in advance. Proportionality is further served by evidence reuse (principle 3.2), by any safe-harbour mechanism the Government chooses to create for importers with robust due-diligence systems, by transition periods, and by ensuring the evidence model is compatible with systems and intermediaries that smaller firms already use. The guiding idea is risk-based escalation rather than universal evidentiary maximalism.

Part 2C, Q8 to Q10 - Commodity differentiation and chain of custody. Evidence requirements should follow a common core with sector-specific extensions rather than a separate evidentiary architecture for each commodity class. For raw materials, extraction or harvest origin, the relevant facility, farm, or site, and custody transfers are the salient elements. For manufactured products, component and input relationships, the supplier hierarchy, and the production facility matter most. For complex, multi-tier goods, the practical approach is risk-prioritized upstream evidence and material-component linkage, with deeper traceability required for inputs identified as high risk. For higher-risk commodities specifically, chain-of-custody evidence should remain associated with the consignment and its relevant inputs through authorized handoffs and transshipment events, rather than being recreated at each system boundary, which is where provenance is most often lost in opaque supply chains. Preserving continuity across those handoffs is an application of principle 3.3.

Part 2D, Q11 - Information sharing and public disclosure. Public disclosure should provide sufficient information on the status and nature of enforcement action to support transparency, predictability, and risk awareness, while keeping underlying confidential evidence subject to applicable legal, privacy, commercial-sensitivity, and source-protection requirements. Beyond that, disclosure design should distinguish clearly between information necessary for public accountability and underlying evidence disclosed confidentially to an enforcement authority. Consistent with principle 3.4, the regime should

protect commercially sensitive supplier relationships, personal information, information whose disclosure could create risks to workers or sources, and security-sensitive information, through minimum-necessary disclosure and role-scoped access. The availability of evidence to a competent authority for enforcement should not, by default, make that evidence public.

5. Technology-Neutral Assessment Criteria

Before any digital traceability infrastructure is relied upon at scale, the Government should define, in advance, what such infrastructure must demonstrate. Pre-specifying evaluation criteria before deployment tests a design's claims rather than documenting favourable outcomes after the fact. The following criteria convert the principles in Section 3 into assessable tests and can be applied to any candidate infrastructure without committing to a particular solution:

- Evidence completeness: can a reviewer obtain the required evidentiary elements for a given consignment?
- Regulator retrievability: can the relevant record for a flagged consignment be retrieved promptly and in structured form?
- Attribution: can material assertions be tied to an identifiable source, actor, and relevant authority or role?
- Integrity and versioning: can alteration and version history be reconstructed?
- Interoperability: can evidence be exchanged across relevant systems without loss of meaning?
- Amendment handling: are prior and current states distinguishable and preserved?
- Selective disclosure: can appropriate evidence be shared without exposing unrelated sensitive information?
- Accountable automation: are consequential determinations reserved to accountable human or institutional authorities, with AI outputs reviewable and logged?
- SME usability: can legitimate smaller importers comply without maintaining bespoke compliance infrastructure?

These are offered as a ready basis for what a defined-scope assessment or pilot of digital traceability infrastructure would need to demonstrate, and how it should be evaluated, should the Government choose to scope one.

6. An Illustrative Canadian Design Approach

To make the preceding points concrete rather than abstract, one Canadian-developed design approach is offered solely to illustrate that the category of infrastructure described above is being actively examined by Canadian practitioners. It is not offered as a recommendation for adoption and is not the subject of this submission.

TransPacific Trade Nexus (TPTN) is a Canada-first, pre-production design-stage approach directed at the structured, attributable, and auditable handling of trade evidence. It is currently at clickable-prototype maturity using synthetic data; no production system, executed pilot, or live integration with any customs or Single Window environment is claimed or implied. Its relevance here should be read against three distinct levels of maturity. At the demonstrator level, the design illustrates audit-event concepts, role-based and read-only institutional interfaces, and an advisory, human-governed interaction pattern, using synthetic data. At the design and pilot-testable level, and not as current operational capability, the broader architecture specifies labour-related and responsible-sourcing evidence handling, stronger participant identity and delegated authority, regulator-grade evidence retrieval, structured cross-system exchange, evidence portability, amendment and version history, exception routing, and evidentiary continuity across handoffs; these are capabilities a pilot would be designed to test, not functions demonstrated today. At the policy level, matters such as a formal government evidence-provenance taxonomy, a common federal evidence architecture, and sector-specific regulatory schemas are recommendations for the regime, not claims about any particular design.

Two points bear emphasis. Responsible-sourcing and labour-related evidence handling have been longstanding design requirements of this architecture, but their implementation remains design-stage and subject to build and pilot validation. And to be unambiguous: TPTN does not detect, and does not determine the presence or absence of, forced labour. Its architecture is designed to support structured handling of relevant evidence, surface documentation gaps and inconsistencies, preserve provenance and

audit history, and route consequential determinations to accountable human or institutional authorities. The example is included only to show that the general evidence, audit, interoperability, and governance characteristics this policy problem requires are already being worked through in a Canadian design context.

7. Recommendations

1. **Establish a common structured evidentiary core.** Define a common structured evidentiary core for information requested under the regime, with risk-based and sector-specific extensions, rather than an open-ended documentary demand.
2. **Require evidentiary integrity.** Require material evidence to carry appropriate provenance, attribution, validity, integrity, and amendment history, so that a verifier can assess not only what is asserted but by whom, under what authority, and whether it has changed.
3. **Design for interoperability and lawful reuse.** Design the regime so that evidence can be reused where legally authorized across complementary Canadian compliance regimes, and exchanged with compatible international systems, while preserving distinct legal tests and decision authority for each regime and avoiding duplicative evidence silos.
4. **Pre-specify technology-neutral testing criteria.** Before relying on digital traceability infrastructure at scale, establish technology-neutral assessment and pilot criteria covering interoperability, auditability, evidence retrieval, attribution, integrity, proportionality, selective disclosure, accountable automation, and SME usability.

This recommendation set is conditional and assessment-oriented by design. It does not recommend any particular provider or procurement decision. It asks the Government to define the evidence and infrastructure characteristics required for effective implementation, and to test them before relying on them at scale.

Respectfully submitted,

Chris Papp

Founder & CEO, TransPacific Trade Nexus (TPTN)

Operating entity: 16422411 Canada Inc. (operating as SynergAI)

Montréal, Québec

References and Notes

[1] Global Affairs Canada and Canada Border Services Agency, *Public consultation on regulatory approach under Bill C-35, An Act respecting the prohibition of the importation of goods produced by forced labour* (2026). Cited for the consultation's scope, questions, tracing-information models, and identified burden-management measures.

[2] Statistics Canada, "Trade by exporter and importer characteristics: Goods, 2023," *The Daily*, May 16, 2024. Reports 163,881 goods-importing enterprises and 48,718 goods-exporting enterprises in 2023.

[3] *Fighting Against Forced Labour and Child Labour in Supply Chains Act*, S.C. 2023, c. 9 (in force January 1, 2024).

[4] UN/CEFACT Buy-Ship-Pay Reference Data Model (trade, transport, and financial data semantics); World Customs Organization Data Model (data content of cross-border regulatory processes). Referenced at the data-semantics and interoperability layer.

[5] UN/CEFACT United Nations Transparency Protocol (UNTP), public review. Contributor comments #672 (Identity Resolution Across the Full Trade-Actor Ecosystem), #673 (Selective Disclosure and Minimum Necessary Data by Transaction Type), and #674 (Auditability and Evidentiary Integrity Across Credential Chains).