December 1, 2026

The Honorable Rodney Scott
Commissioner
U.S. Customs and Border Protection
Department of Homeland Security
Washington, DC

Re: Joint Association Letter – Heightened Import Disclosures for Supply Chain Visibility (Docket No. USCBP-2026-1058)

Dear Commissioner Scott:

The undersigned associations, representing companies of all sizes across a broad range of sectors, appreciate the opportunity to comment on U.S. Customs and Border Protection's (CBP) advance notice of proposed rulemaking (ANPRM), "Heightened Import Disclosures for Supply Chain Visibility." We support CBP's goal of strengthening enforcement of U.S. customs and trade laws, including efforts to identify illicit imports, illegal transshipment, duty evasion, and other conduct by bad actors that undermines compliant businesses and the integrity of the U.S. trading system.

At the same time, any new requirements should be carefully tailored to produce actionable enforcement benefits without imposing broad, duplicative, or impracticable obligations on legitimate trade. The overwhelming majority of importers invest substantial resources in compliance and should not bear disproportionate costs because of misconduct by a limited number of bad actors. CBP should therefore preserve a risk-based approach, direct heightened scrutiny toward shipments, entities, commodities, and trade lanes presenting demonstrable risk, and provide streamlined treatment for trusted and consistently compliant companies.

Foreign Export Documentation and Data Availability

CBP should recognize that U.S. importers may not possess, control, or have a legal right to obtain documents filed by a foreign exporter with its customs authority. Depending on the country, such records may be held by the exporter, a broker, a carrier, or the foreign government; may contain confidential commercial or personal information; and may be subject to data-localization, privacy, secrecy, licensing, or other legal restrictions. Document formats, terminology, filing systems, retention periods, and access rights also vary significantly across jurisdictions. In most cases, an American importer will have no means of validating the authenticity of this documentation. An importer should not be penalized for failing to produce information that it does not control, cannot lawfully obtain after undertaking reasonable efforts and cannot verify.

In addition to the issue of limited access, there are a myriad of reasons why foreign export filings may not align directly with U.S. import declarations and thus would not serve to evaluate the accuracy of U.S. import declarations. Other countries have different non-

preferential origin regimes, which may yield a different country of origin. Other countries may take a different position on tariff classification. Methodologies to determine valuation may also vary by country. The foreign country may require a certain type of registration for an entity to act as exporter, so the exporting party may not match the manufacturer declared on import into the U.S. These are but a few examples why foreign export declarations do not serve to validate information declared on import into the U.S.

The cost of obtaining this documentation and managing storage and submission is substantial. Given the limited enforcement value of unverified information, industry resources would be better focused on other security and compliance measures.

CBP has built strong relationships with foreign customs administrations, sharing a desire to counter bad actors and safeguard each nation's security, and is better positioned to request records directly from other government agencies. If CBP is unable to negotiate such arrangements, private-sector actors are even less likely to be successful. Rather than shifting responsibility for foreign-government records to U.S. importers, CBP should work directly with foreign counterparts to develop lawful, secure, and interoperable mechanisms for obtaining and validating appropriate data, while safeguarding commercially sensitive information. Further, it is likely that foreign governments will enact reciprocal requirements to request commercially sensitive information from U.S. companies, potentially undermining U.S. competitiveness and supply chain security.

Importers should not be required to certify the accuracy of foreign filings they did not prepare and cannot independently verify, and cargo release should not be conditioned on the transmission of records from a foreign government or other third party outside the importer's control. Any future rule should permit reasonable alternatives when a requested foreign document is unavailable, accept data elements or verification results in lieu of full documents where sufficient for enforcement, protect business-confidential information, and establish clear safe harbors based on reasonable care and documented good-faith efforts. CBP and industry could test the cost-benefit analysis of this data collection through targeted pilots and ensure that a reasonable timeline accompanies rollout. Ultimate efforts should be limited to recordkeeping, and not required for routine entry filing, given the substantial cost of such data collection.

Proportionality, Small Business Impacts, and Implementation

Before proposing specific requirements, CBP should identify the enforcement problem each new data element is intended to address, determine whether CBP already receives the information from another source, and assess whether the expected benefit justifies the cost. Requirements should be standardized, technology-neutral, and limited to data that are necessary and reasonably available in the ordinary course of business. CBP should avoid duplicative submissions, unnecessary retention mandates, and one-size-fits-all obligations that do not account for differences among industries, business models, supply chains, shipment types, and countries of origin. The cost-benefit calculation should take into consideration the commercial value of this data, which will likely include trade secrets that underpin the competitiveness of American industry.

CBP should reuse and reconcile information already available through ACE, entry filings, Importer Security Filings, manifests, and other government systems before requiring a trade participant to submit the same or substantially similar information again. Information should be collected once, from the party best positioned to provide it, and reused for authorized customs purposes where practicable.

Any required identification of manufacturers, producers, facilities, exporters, shippers, marketplaces, or other supply chain parties should be based on clear functional definitions tied to the relevant customs purpose. CBP should evaluate existing government and industry identifiers before creating a new mandatory identifier and should favor open, interoperable, low-cost approaches over dependence on a limited number of proprietary systems.

Origin verification requirements should also reflect the realities of multi-source commodity and manufacturing supply chains. CBP should not require importers to designate a single "primary" or "secondary" source when several sources are used interchangeably, and the importer cannot accurately rank them. Where sources receive identical tariff treatment and present equivalent enforcement risk, CBP should consider appropriately defined origin categories or other flexible reporting methods, supported by records demonstrating the exclusion of restricted or specially treated sources.

These considerations are especially important for small and medium-sized businesses, which have less leverage over foreign suppliers and fewer personnel and systems available to absorb new compliance obligations. CBP should conduct a rigorous assessment of direct and indirect costs, consider tiered or risk-based requirements and appropriate exemptions or simplified procedures, and ensure that small businesses have access to clear guidance, training, and technical assistance.

Technology Neutral Approach, Voluntary Pilots, Avoiding Vendor Lock-In

Supply chain mapping, tracing, and risk analysis technologies contribute to improved enforcement, but they should supplement rather than displace CBP's responsibility to collect, aggregate, validate, and analyze information available to the government. CBP should not require importers to provide unrestricted access to proprietary systems, sourcing information, or supplier networks, or make importers responsible for independently reconstructing information that government authorities or other supply-chain parties are better positioned to obtain.

Before mandating a particular tracing capability, platform, identifier, or technology standard, CBP should conduct voluntary pilots to evaluate accuracy, reliability, cost, interoperability, cybersecurity, and incremental enforcement value. Any resulting standards should remain technology neutral, should not favor particular vendors or business models, and should allow secure submission of relevant data, findings, or verification results.

CBP should also consider a voluntary, non-exclusive framework under which importers may rely on documented findings or verification results from qualified independent providers as one means of supporting reasonable care. Any such framework should use transparent and

objective eligibility criteria, allow participation by any provider that meets those criteria, preserve alternative methods of substantiation, make clear the use of a third-party provider is not required to demonstrate reasonable care, and avoid requiring the use of a particular vendor, platform, or proprietary technology. Reliance on a qualified provider should not transfer CBP's enforcement responsibilities to the private sector or prevent CBP from conducting targeted verification where warranted.

Preserve the Voluntary Nature and Value of CTPAT

The Customs Trade Partnership Against Terrorism (CTPAT) is an important voluntary public-private partnership to support supply chain security and facilitate legitimate trade. CTPAT participants make continual and substantial investments in personnel, systems, documentation, supplier oversight, physical security, cybersecurity, validation preparation, and corrective actions—often exceeding the baseline obligations applicable to nonparticipants. Those investments were premised on a voluntary partnership in which enhanced security commitments would be matched by meaningful, predictable, and measurable facilitation benefits. It is critical, therefore, that the U.S. government continues to invest and enable the program to help CBP "reduce the size of the haystack" while searching for threats. CBP should also avoid using new supply chain transparency requirements in a manner that makes CTPAT participation effectively mandatory.

CBP should avoid making this program more burdensome given the already-significant cost of participation. At the same time, there needs to be greater consistency and visibility into the benefits participants receive. Participants are increasingly facing the same examinations, holds, documentation demands, and operational disruptions as nonparticipants; stated benefits may be unavailable at particular ports, inconsistently applied, or outweighed by new compliance expectations; and companies have limited visibility into whether their CTPAT status materially improves cargo processing. A program cannot remain a credible voluntary partnership if obligations continue to expand while benefits become uncertain, discretionary, or largely indistinguishable from those afforded to nonparticipants.

CBP should not rely on CTPAT membership as the principal means of obtaining relief from new regulatory burdens without providing concrete, consistent, and transparent benefits commensurate with the cost of participation. Otherwise, companies would be compelled to join not because the program offers a compelling security-and-facilitation partnership, but simply to avoid a competitive disadvantage—effectively making CTPAT mandatory without the safeguards, analysis, and accountability that should accompany a regulatory requirement.

This concern is particularly acute for smaller importers and customs brokers. These businesses may lack the dedicated compliance staff, bargaining power over foreign suppliers, and financial and technological resources needed to complete the application process and maintain program requirements. CBP should not establish a two-tier commercial environment in which smaller entities face materially greater costs or delays simply because CTPAT participation is not practicable for them. The agency should preserve viable risk-based pathways for non-CTPAT companies, improve and clearly define benefits for participants, and consider

proportionate or graduated participation options that make the program genuinely accessible to smaller businesses.

CBP must also ensure that it has sufficient personnel and resources to conduct timely validations and revalidations for importers and brokers of all sizes. Expanding reliance on CTPAT without a corresponding increase in validation capacity could create lengthy backlogs, disadvantage smaller applicants, and prevent qualified companies from obtaining promised benefits. Before linking any new regulatory relief or compliance expectations to CTPAT status, CBP should publish service standards, assess anticipated application and validation volumes, dedicate adequate staffing and funding, and demonstrate that it can administer the program fairly and consistently.

Implementation timelines

A realistic implementation period is essential to effective enforcement. Companies will need time and resources to obtain and validate data across multiple supplier tiers, address foreign-law and contractual constraints, deploy traceability technologies, establish interoperable standards, integrate systems, train suppliers, and test data flows. These steps are sequential and resource-intensive; a compressed deadline would produce unreliable submissions, disrupt compliant trade, and burden CBP with data that weakens rather than improves targeting.

CBP should use a milestone-based rollout: publish final technical requirements before the compliance clock begins, conduct pilots, phase requirements by data complexity and business readiness, and provide an informed-compliance period for good-faith corrections. Mandatory enforcement should begin only when both industry and CBP have the systems, staffing, funding, training, and cybersecurity safeguards needed to implement the rule reliably. This approach would protect lawful commerce while advancing CBP's enforcement objectives.

CBP Resources and Continued Stakeholder Engagement

Additional data will improve enforcement only if CBP has the personnel, technology, cybersecurity safeguards, analytical capacity, and training needed to evaluate and act on it. CBP should assess these resource needs before imposing new collection requirements and should coordinate with Congress and the Department of Homeland Security to secure adequate funding. The agency should also explain how new information will be integrated into targeting systems, measured for utility, protected from unauthorized disclosure, and reviewed to eliminate data elements that do not materially improve enforcement outcomes.

Continued partnership with the trade community will be essential. CBP should consult regularly with importers, exporters, customs brokers, carriers, technology providers, small-business representatives, and the Commercial Customs Operations Advisory Committee throughout rule development and implementation. Structured working sessions, pilots, technical demonstrations, and publication of draft data specifications would help CBP identify operational and legal barriers early and design requirements that are workable across diverse supply chains.

Conclusion

We urge CBP to pursue a focused, risk-based framework that strengthens action against bad actors while facilitating lawful commerce. Any future proposal should be supported by a clear enforcement rationale, account for foreign-law and data-access constraints, minimize burdens – particularly for small businesses – provide adequate time and safeguards for implementation, and ensure that CBP has the resources necessary to achieve its objectives. The undersigned associations stand ready to work with CBP to advance these shared goals.

Sincerely,