October 17, 2025

Cathy Gautreaux
Office of Multimodal Freight Infrastructure and Policy
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Re: Docket No. DOT-OST-2025-1326

Dear Ms. Gautreaux:

On behalf of the Intermodal Association of North America (IANA), the leading transportation trade association representing the combined interests of the intermodal freight industry, I am writing to share our response to the Request for Information on "Protecting America's Supply Chain from Cargo Theft," Docket No. DOT-OST-2025-1326.

IANA's membership roster of over 1,000 corporate members includes intermodal and over-the-road motor carriers, as well as railroads (Class I, short-line, and regional), water carriers, port authorities, intermodal marketing and logistics companies, and suppliers to the industry such as equipment manufacturers, leasing companies, and technology firms. IANA's associate (non-voting) members include shippers (defined as the beneficial owners of the freight being shipped), academic institutions, government entities, and non-profit trade associations.

Your attention to this growing challenge is well timed and much appreciated. This summer, IANA surveyed its membership to gain insight into the impact of cargo theft on our industry. The results showed that 76 percent of respondents are more concerned with cargo theft today than five years ago and 53 percent of respondents have been impacted by cargo theft. Cargo theft is trending in the wrong direction and wreaking havoc on our nation's supply chains.

We appreciate your leadership on this important effort and your support for intermodal goods movement. IANA looks forward to working with you and would welcome the opportunity to further engage with your office. If you or your staff have any questions, please do not hesitate to contact me at areinke@intermodal.org or 301-982-3400.

Sincerely,

Anne C Reinke

Anne Reinke
President and CEO
Intermodal Association of North America

Request for Information:
Protecting America's Supply Chain from Cargo Theft

1. What are the most significant cargo theft risks facing the U.S. supply chain today (*e.g.,* opportunistic thefts, organized theft rings, insider threats, cyber-enabled diversion)?

As 95% of all manufactured goods move at one point or another on the supply chain in a container, the intermodal freight industry invests heavily in technologies and capabilities to reduce cargo theft.

The most significant risks facing U.S. supply chains come in the form of strategic and highly sophisticated schemes – including organized theft rings/international crime cartels, insider threats, and cyber-enabled diversion. These schemes present complex challenges and require strong partnerships with law enforcement. As industry works hard to deter theft and stay ahead of criminals, thieves continue to innovate, with new tactics and targets emerging constantly. The financial loss is estimated to be billions of dollars each year, and the public safety threat from organized cartel activity is immense. For example, blocking rail rights of way or otherwise using unsafe means to stop a train could have potentially devastating impacts to surrounding communities should a derailment occur.

The increase in cybercrime is not unique to the freight sector, however, its impacts on supply chain reliability and safety are significant. Through double brokering scams, identity theft, or falsified bills of lading, criminals can misdirect or steal entire shipments without the high risks of physical intervention. To effectively deter these crimes, industry efforts must be supported by timely law enforcement intervention, clear and consistent legal consequences, and improved coordination across federal, state, and local jurisdictions.

Opportunistic and straight theft remain a significant threat, especially when cargo is idle at truck stops, parking lots, warehouses, or on stopped trains. The security of transportation workers, drivers and the public is put at great risk by robberies which have taken on more sophistication. These types of cargo theft are tragically common and underreported. The financial impacts are significant with the estimated average value of individual theft at greater than $202,000.

2. How do these risks vary across different types of goods movement: truck borne freight, rail borne freight, water borne freight, air borne freight, and freight located at multimodal exchange points, including airports, marine ports, and truck-rail intermodal facilities?

Cargo theft can take many different forms. Stationary and slow-moving cargo is particularly vulnerable, making rail yards and intermodal transfer facilities targets. By design, intermodal freight supply chains are comprised of multiple modes and points of transfer, reflecting the most efficient use of each mode. This allows the industry to combine the strengths of rail, maritime, and road transportation to deliver goods quickly, safely, and cost effectively. However, the same qualities that make intermodal transportation so effective also leave these movements vulnerable to theft. This vulnerability, paired with knowledge that intermodal containers often carry consumer goods with resale value, makes intermodal freight a target.

Risks across different types of goods movement may vary due to each mode or facility's unique security and access restrictions that are already in place for reasons unrelated to cargo theft. For example, following the terrorist attacks on September 11, 2001, advanced security enhancements were introduced to limit access to maritime facilities. Specialized credentials are required for workers to enter these facilities, reducing the risk of theft by unauthorized individuals. These facilities also host federal law enforcement agents from Customs and Border Protection and the Transportation Security Administration. Accordingly, theft is more likely to occur when freight moves through unrestricted routes or facilities.

3. For each of the following modes of transportation, please indicate how much of a challenge cargo theft is for shippers and carriers.

It is challenging to assess the risk of cargo theft by mode alone. While we recognize that a form of classification may be necessary, there are vulnerabilities that extend beyond modes of transportation to nodes or facilities (e.g., warehousing), particularly considering the interconnected nature of freight supply chains. For example, using the classifications below, cargo theft in marine transportation could refer only to vessels at sea, which may be vulnerable to piracy in international waters. However, it could also be viewed as instances of cargo theft after the goods have left the vessel and are staged in or around port facilities. Likewise, theft occurring at a warehouse or transfer facility could involve trucking and/or rail, making it difficult to quantify. Finally, also notable is that the theft of chassis creates overall supply chain dysfunction. We encourage DOT to consider these unique multimodal aspects as the Department further refines its approach.

IANA has included its ratings for each mode below:

Mode	5 (Very Serious)	4	3	2	1 (No Challenge)	N/A
Air	☐	☐	☐	☐	☐	X
Rail	X	☐	☐	☐	☐	☐
Marine	☐	☐	X	☐	☐	☐
Trucking	X	☐	☐	☐	☐	☐

4. What barriers prevent timely detection, reporting, and response to cargo theft incidents? How can DOT reduce these barriers?

A major barrier to the timely detection and effective response to cargo theft is the lack of accurate and centralized data. Cargo theft is widely underreported for a host of reasons, including reputational brand management, tedious paperwork, and the low cargo recovery rate. As a result, the actual impact of cargo theft at the national level is difficult to determine, with loss estimates ranging from $455 million to over $35 billion annually.

Inconsistent protocols and confusion surrounding investigation and enforcement authority further contribute to the underreporting of cargo theft and a lack of accurate data on these instances. Currently, there is no definition in federal law for the term "cargo theft," and each state uses varying definitions and procedures to investigate and prosecute these crimes. Additionally, the interstate nature of freight transportation can make it difficult to identify where the theft occurred as well as the appropriate jurisdictional authority. These factors can prevent law enforcement and industry from identifying broader patterns, such as organized theft rings that operate across state boundaries.

DOT can play an important role in reducing these barriers by supporting a more standardized, national approach to cargo theft reporting and data sharing. Improved coordination among federal (for example, DOT, FBI, DEA, ATF and DOJ), state, and local law enforcement, coupled with real-time information sharing with industry, would strengthen detection and response.

5. How can Federal, State, and local law enforcement better coordinate to address both opportunistic thefts and multi-jurisdictional organized cargo theft cases?
   – *AND* –
6. What role should Federal intelligence functions play in identifying and mitigating theft risks across this spectrum?

Congressional proposals to address cargo theft, such as the Combating Organized Retail Crime Act (H.R. 2853 and S. 1404 and the Household Goods Shipping Consumer Protection Act (H.R. 880 and S. 337) would offer further tools and resources to aid federal agencies in reducing instances of supply chain crime.

Pertaining to DOT specifically, the Household Goods Shipping Consumer Protection Act would expand Federal Motor Carrier Safety Administration (FMCSA) authority to identify bad actors during the registration process before fraud occurs and act swiftly to penalize fraudulent companies. By strengthening enforcement of anti-fraud and consumer protection laws, the legislation will increase accountability and support reputable businesses in the shipping industry, improving overall supply chain safety. IANA commends the FMCSA for commencing the modernization process of their motor carrier registration system, as well as their National Consumer Complaint Database. Their efforts will surely result in higher prevention of fraudulent and unsafe carriers from entering and staying on the supply chain.

IANA supports the Combating Organized Retail Crime Act (CORCA), which takes several steps to address existing gaps in the detection and response to cargo theft. Among other provisions, the legislation would establish the Organized Retail and Supply Chain Crime Coordination Center within Homeland Security Investigations at the Department of Homeland Security. The Center seeks to improve coordination between federal, state, and local law enforcement agencies, facilitate partnerships with private sector stakeholders, enhance information sharing, and track trends in organized supply chain crime. A centralized federal Coordination Center is uniquely positioned to aggregate data, identify trends that may not be visible at the local level, and disseminate timely information to both law enforcement and industry partners.

Increased coordination, communication, and data sharing across all levels of law enforcement are particularly crucial in addressing organized cargo theft as these crimes are more likely to occur across jurisdictional boundaries. Federal intelligence agencies will play an important role in identifying cross-jurisdictional and international crime rings, whose activities and networks may extend beyond cargo theft to other types of crimes. Federal entities are best positioned to investigate and prosecute these criminals.

We recognize that law enforcement entities are resource-constrained and often forced to make difficult decisions as to which crimes to prioritize and pursue. Cargo theft is often treated as a property crime at the local level, which makes it a lower priority and does not account for the significant safety risks to supply chain workers. Increased education, training, and awareness of the issue can help mitigate threats and improve workforce safety for essential workers across the multimodal freight system.

7. How should DOT Operating Administrations (FMCSA, FHWA, FRA, MARAD, FAA, and PHMSA) contribute to addressing cargo theft while avoiding duplication of FBI/DHS roles?

DOT's Operating Administrations can play an important role in addressing cargo theft by focusing on prevention, coordination, and stakeholder engagement, while leaving direct criminal investigation and enforcement to the FBI, DHS, and other law enforcement agencies. Each OA brings unique modal expertise and industry relationships that, when coordinated, can help identify vulnerabilities, promote best practices, and support investments that reduce exposure to theft. There are various physical deterrents and safety enhancements that can be incorporated into projects under each modal agency. For example, FHWA can encourage projects that include safety improvements in truck parking facilities. Likewise, MARAD and FRA can promote enhanced terminal, yard, and cyber security protocols. FMCSA has unique opportunities to identify potential strategic cargo theft and fraud offenders throughout its registration systems and databases.

8. What data collection improvements (e.g., reporting platforms, integrations with FMCSA inspections or CBP data) should DOT pursue to enhance cargo theft visibility?

As discussed extensively in this response and elsewhere, cargo theft is gravely underreported. There are several reasons for this. A uniform definition of "cargo theft" and a central repository for reporting would go far in illuminating this growing issue. IANA supports CORCA and its centralized federal Coordination Center that can aggregate data and identify trends that may not be visible at the local level. Data sets from many sources will be necessary to inform this Center.

As mentioned, IANA supports the Household Goods Shipping Consumer Protection Act. The legislation would expand FMCSA's authority to identify bad actors during the registration process before fraud occurs and act swiftly to penalize fraudulent companies. Information on these bad actors would be valuable to the Center. Likewise, CBP plays an important role in the fight against cargo theft at our international gateways. CBP data would be highly valuable to the Center and its mission to identify national and international cargo theft trends and sophisticated crime rings.

9. Are there regulations that cause or contribute to vulnerabilities that lead to cargo theft?

The lack of a clear and consistent definition at the federal level of "cargo theft" makes it more challenging for both industry and law enforcement to identify, report, and respond to instances of cargo theft. Without strong enforcement and legal consequences, criminals will see cargo theft as a low-risk, high-reward crime.

10. What industry best practices or technologies (e.g., GPS tracking, electronic seals, AI-driven monitoring, secure parking, etc.) have proven most effective in reducing both opportunistic thefts and organized thefts?

The intermodal industry is steadfast in its commitment to deter cargo theft and has voluntarily adopted several practices and technologies to discourage criminals. Over the summer of 2025, IANA polled its membership to gain insight into the industry impacts of cargo theft. Nearly 60 percent of respondents have invested resources in cargo theft prevention and detection efforts. These responses detail a multilayered approach to security, meaning technology, physical barriers, route modifications, and human guards are in place to deter, prevent, and interrupt cargo theft.

Intermodal containers are frequently equipped with global positioning systems (GPS) or radio-frequency identification (RFID) tags that provide location tracking, but unfortunately, thieves often use GPS jamming devices to interrupt tracking. Containers can also be equipped with advanced locks, seals and door sensors that detect unauthorized openings and alert shippers. Sadly, our members report that thieves have used heavy-duty equipment to cut and enter containers from the top or sides. Our members have also reported that advanced locking systems can serve as a visual cue to thieves that the container contains high-value goods. Shippers take steps to organize containers such that high-value goods are more difficult to access, and likewise, thieves have caught on to this. The industry continues to invest and innovate in solutions, but unfortunately, criminals have been quick to learn and adapt accordingly.

While industry can deter criminals, it is law enforcement's responsibility to identify and charge them with crimes. Theft, fraud, and cyber-security attacks aimed at freight transportation will require a host of solutions.

11. How should DOT measure success in reducing cargo theft, and what performance metrics would be most valuable to track?

Cargo theft is underreported. Inconsistent protocols and confusion surrounding investigation and enforcement authority contribute to the underreporting of cargo theft and a lack of accurate data on these instances. In its member survey concerning cargo theft's industry impacts earlier this year, 14 percent of respondents reported cargo theft to the FBI tip line; 60 percent reported theft to state or local law enforcement; and 57 percent reported the theft to their insurer (respondents were able to select all applicable options). Over 11 percent of respondents did not report the theft at all.

To measure the success in reducing cargo theft, a consistent reporting protocol and definition are necessary. At a minimum, performance metrics should track the value, frequency of occurrence, geographic location, commodity, and mode/node. These metrics would not only track trends, but they would also illuminate the most vulnerable transactions and locations in our supply chain.

12. To what agency or jurisdiction does industry currently report cargo theft? What barriers prevent industry from reporting theft incidents to Federal agencies? How can DOT reduce these barriers?

Companies impacted by cargo theft have reported the theft to a number of different entities, including state and local law enforcement, the FBI tip line, and insurance carriers. Underreporting due to brand management concerns and jurisdictional confusion remain significant concerns. DOT can assist in reducing these barriers by raising awareness of cargo theft and appropriate reporting methods through its communications tools and educational materials.

13. Which commodities face the highest risks and do those risks vary contingent on whether the commodity is domestic, imported, or exported?

It is difficult to map clear trends on this due to the disjointed reporting process, but there are many markers and anecdotes available. According to CargoNet, thieves frequently target food and beverage shipments. Consumption of these products reduces the ability of law enforcement to trace crimes. Our members have also shared instances of high-value, large item theft. For example, one of our members shared that a truck was stolen and used to enter a secure facility in St. Louis, Missouri to take two containers holding high-end refrigerators. The refrigerators turned up several months later when the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) conducted a raid on a warehouse in a St. Louis suburb. The refrigerators were located with their back cavities removed and cash stuffed inside. They were being used to smuggle money across the southern border.

14. What potential practices, technologies, or focal points for investigation could DOT initiate over the next year to test innovative approaches to cargo theft prevention, reporting, and enforcement partnerships?

The Freight Logistics Optimization Works (FLOW) initiative is a valuable tool for participants to track, access, and share real-time supply chain data. Due to the established set of supply chain metrics and diversity of stakeholders participating in the program, we encourage DOT to explore opportunities to integrate metrics related to cargo theft into FLOW. The anonymous nature of the data collected through FLOW may also result in more accurate estimates of the number of thefts and its economic impact occurring across the country.