



October 19, 2025

United States Department of Transportation
Office of the Secretary
Cathy Gautreaux, Deputy Assistant Secretary
Office of Multimodal Freight Infrastructure and Policy
1200 New Jersey Avenue, SE
Washington, DC 20590

Subject: Docket No. DOT–OST-2025–1326 – Response to the Protecting America’s Supply Chain from Cargo Theft –Request for Information (RFI)

Dear Deputy Assistant Secretary Gautreaux,

The Retail Industry Leaders Association (RILA) welcomes the opportunity to respond to the U.S. Department of Transportation’s (DOT) Request for Information on cargo theft, a growing risk that endangers supply chain integrity, public safety, and economic resilience.

RILA is the U.S. trade association for leading retailers. We convene decision-makers, advocate for the industry, and promote operational excellence and innovation. Our aim is to elevate a dynamic industry by transforming the environment in which retailers operate. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than \$2.7 trillion in annual sales, millions of American jobs, and hundreds of thousands of stores, manufacturing facilities, and distribution centers.

As the voice of leading retailers, RILA’s member companies operate complex, high-volume supply chains that are increasingly targeted by opportunistic and organized theft operations. Our members face evolving threats across transportation modes and facilities, and have invested heavily in technologies, protocols, and partnerships to mitigate risk.

Organized retail crime remains a persistent and growing challenge for the industry. In-store incidents, such as coordinated smash and grab thefts, continue to disrupt operations and endanger employees and customers. Additionally, the rise in gift card fraud and other financial schemes reflects the increasing sophistication of criminal networks targeting retailers. These activities are often linked to broader organized crime groups that also engage in cargo theft, cyber-enabled diversion, and fraudulent logistics operations. Cargo theft has proliferated in recent years and reflects growing involvement by organized crime networks, though the groups behind straight cargo theft attacks are generally distinct from the groups perpetrating strategic cargo theft

attacks. In many cases, these networks are connected to other serious criminal enterprises, including human, drug, and weapons trafficking, as well as terrorism financing.

Both straight and strategic cargo theft have surged in recent years, with each year setting new records for frequency of incidents and financial value of lost merchandise and affected operations. Strategic cargo theft alone grew nearly 1,500% since 2021. As large as the existing numbers are, nearly all stakeholders agree that due to challenges in tracking and reporting, industry data does not reflect the full scale of the cargo theft problem.

Cargo theft is not only a supply chain issue but also a public safety and economic concern that intersects with organized crime, cyber-enabled fraud, and cross-jurisdictional criminal networks. RILA strongly supports the Combating Organized Retail Crime Act (CORCA)¹, a legislative framework designed to enhance federal coordination, data sharing, and enforcement strategies across jurisdictions. While not focused exclusively on cargo theft, CORCA addresses the broader infrastructure of organized retail crime, including the illegal acquisition and movement of goods, which frequently intersects with freight crime. The bill's provisions for interagency collaboration, centralized enforcement, and intelligence sharing offer a critical foundation for addressing the systemic challenges retailers face.

This response reflects input from a broad cross-section of RILA members, including retailers, logistics providers, and supply chain security experts. It outlines key risks, barriers, and opportunities for collaboration, and offers recommendations for how DOT can enhance its role in cargo theft prevention, reporting, and enforcement.

Most Significant Cargo Theft Risks

Cargo theft has dramatically increased in recent years. A survey of RILA members found that over half of respondents experienced increased strategic cargo theft over the previous 24 months (with 28% reporting a “significant” increase), and two-thirds experienced increased straight cargo theft (23% reporting a “significant” increase). Average losses per incident totaled 3 to 5 million dollars, and more concerning were the safety risks: a third of all respondents experienced armed violence in the commission of thefts.

- Straight cargo theft continues to be a significant issue for RILA members, with burglary and opportunistic theft reported as the most prevalent (86% of respondents) and rail theft (65% of respondents) similarly pervasive. Members emphasized the vulnerability of distribution centers, warehouses, and container yards, where thefts often occur due to insufficient physical security and limited surveillance. Additionally, cargo left unsecured at rest during transit—such as in truck yards or rest stops—is frequently targeted by opportunistic criminal elements. Shortages of safe, secure truck parking for drivers in transit also contribute to this vulnerability.

¹ U.S. Congress. (2025). *S. 1404 — Combating Organized Retail Crime Act*. 119th Congress. Retrieved from <https://www.congress.gov/bill/119th-congress/senate-bill/1404>

- Straight theft like this occurs throughout the country, however members described a troubling pattern of hotspots that are transfer points or areas of high cargo density, such as Southern California, Dallas/Fort Worth, Phoenix Memphis, Chicago, Atlanta, coastal New York / New Jersey, and to a lesser extent Houston and locations in Florida.
- Members report rail theft to be particularly acute in certain geographic areas, including coordinated thefts along the Southwest transportation corridor, and major rail yards or transfer points. Criminal organizations are targeting retail freight in high-traffic areas nationwide, using increasingly sophisticated methods to intercept and divert shipments. This reflects a broader trend of organized theft that is impacting retailers throughout the United States.
- RILA members consistently identify strategic cargo theft, particularly attacks carried out by organized crime groups, as one of the most pressing threats to the U.S. retail supply chain. While both straight and strategic theft numbers are growing, strategic theft is increasing at a sharper pace and can be more challenging to tackle due to the dispersed threat of cyber bad actors and theft rings operating from countries around the world. Strategic theft schemes include unauthorized double-brokering (and sometimes triple-brokering), identity theft, motor carrier (MC) number transfer and misuse, fraudulent/doctored bills of lading (BoLs), and fictitious pickups.
- Strategic theft alone increased 1,500% since 2022, according to CargoNet². Members noted firsthand experience with the sharp increase in fictitious pickups, where fraudulent entities use counterfeit documentation to gain access to loads, and then disappear with the goods. The ease with which bad actors are able to obtain MC numbers has long enabled the prevalence of strategic theft, which the FMCSA has made moves to address through modernization of its registration system. Members highlighted that load boards, while useful for freight matching, have become a tool for bad actors to impersonate legitimate carriers. This impersonation is sometimes unintentionally facilitated by inadequate vetting practices among brokers, who may lack the tools or protocols to verify carrier legitimacy.
- Additionally, some members reported incidents involving hacked carrier communications, drivers being paid to divert shipments, and the purchase or misuse of motor carrier (MC) numbers to create false identities. The use of counterfeit paperwork

² Verisk CargoNet: Cargo Theft Isn't a Trucking Problem. It's a National Crisis. <https://www.trucking.org/news-insights/cargo-theft-isnt-trucking-problem-its-national-crisis#:~:text=While%20it%20made%20for%20gripping,shows%2C%20no%20one%20is%20immune>

(including BoLs) and fake identification to gain access to freight facilities or facilitate partial theft was also cited as a significant concern.

There is a need for stronger coordination between federal, state, and private sector stakeholders, as well as enhanced enforcement tools to address the growing threat of organized retail crime. RILA believes these challenges can be effectively addressed through the provisions of the CORCA, which seeks to improve federal response to organized retail crime by:

- Facilitating interagency collaboration between the Department of Homeland Security, Department of Justice, and other relevant agencies.
- Establishing a coordinated federal enforcement center to investigate and prosecute organized retail crime networks.
- Enhancing data sharing and intelligence gathering across jurisdictions and sectors.
- Supporting efforts to dismantle criminal enterprises that traffic in stolen retail goods, including those operating through online marketplaces and cargo theft fencing and resale schemes.

Risk Variation Across Transportation Modes

RILA members also report significant variation in theft vulnerability across transportation modes. Members noted that truckload freight accounts for the highest volume of shipped retail goods compared to other modes. It is particularly vulnerable to both direct theft, such as hijackings and burglaries, and strategic theft, including identity fraud and fictitious pickups. Meanwhile for RILA members rail freight is primarily affected by straight theft, whether opportunistic or targeted, often occurring at major interchange points where intermodal containers are breached, and especially in areas with limited physical security infrastructure.

Airborne freight, while less frequently used by retailers, has experienced isolated thefts. Due to the relatively costly nature of air freight, merchandise shipped by air is frequently of higher importance and has a higher value or larger margin. However, due to the relatively low volume of goods shipped via air, the impact of these incidents is not as broadly significant across the industry.

Marine freight was generally considered lower-risk, though some noted isolated incidents, typically involving containers in port or port-adjacent facilities with less oversight. Thirty-two percent of RILA members surveyed reported experiencing thefts of or from containers within port boundaries.

Multimodal exchange points such as airports, marine ports, and truck-rail intermodal facilities were identified as areas of concern, particularly in situations where coordinated security protocols or infrastructure are lacking. In some cases, strategic partnerships have been formed in

multimodal lanes. While these partnerships were not originally designed with security in mind, they have nonetheless improved visibility and accountability, providing a security advantage.

While CORCA was developed to address organized retail crime, its emphasis on enforcement coordination and intelligence-sharing is highly applicable to the growing threats across modes and across the entire supply chain, including cargo theft. These provisions can help strengthen prevention efforts—particularly at vulnerable multimodal exchange points where organized criminal activity often overlaps with freight movement.

Cargo Theft Challenge Ratings by Mode

RILA members provided ratings to reflect the severity of cargo theft across various transportation modes. Rail freight was consistently identified as one of the highest-risk areas, with members rating it between 4 and 5 on a five-point scale, citing frequent incidents at major interchange points and vulnerabilities in container security. Air freight received mixed ratings, ranging from 2 to 4, indicating moderate to serious concern. While incidents do occur, the relatively low volume of air shipments limits the overall impact.

Trucking was rated between 2 and 5, reflecting a wide range of experiences. While not all retailers utilize air freight or rail/intermodal, all retailers move at least some goods by truck. While some companies reported only minor issues, many others described serious challenges, particularly related to theft during transit and at unsecured rest locations. Furthermore, trucking is more exposed to personal safety concerns, where drivers may be alone and vulnerable to armed hijacking of loads.

Marine freight, by contrast, was generally considered lower risk, with ratings between 1 and 2, suggesting minimal concern among most respondents.

In addition to the modes listed in the RFI, members highlighted other areas of vulnerability. Distribution centers, warehouses, and third-party yards were rated as a challenge, primarily due to gaps in physical security and access control. Parcel fraud, involving manipulated delivery data or false claims, was also rated as an issue. Package theft, especially in the final mile of delivery and including porch piracy, was considered a moderate challenge, reflecting its growing prevalence in e-commerce logistics.

Across all modes and facilities, members consistently pointed to the role of physical infrastructure, technology, and operational protocols in shaping risk levels. Locations with limited security, such as unsecured truck yards or parking lots, were repeatedly cited as high-risk environments. These challenges suggest that improving security standards and operational oversight across freight modes and facilities could significantly reduce exposure to straight cargo theft.

Barriers to Detection, Reporting, and Response

RILA members identified several persistent barriers that hinder timely detection, reporting, and response to cargo theft incidents. Cargo theft can be challenging to detect and identify due to the inherent complexity of supply chains, which involve multiple parties and frequent transfers of goods. Depending on contract terms and other factors, at various points in cargo's journey from origin to customer, it can be in the possession of manufacturers, wholesalers, carriers, third-party providers, and other stakeholders. Members reported that the complexity of the supply chain can mean thefts may go undetected for extended periods, sometimes days or even weeks, making it difficult to determine when and where the loss occurred. Furthermore, fraudulent or doctored documentation such as BoLs make it challenging to identify a single source of truth and detect loss or shortages. The absence of standardized security protocols and clear communication expectations between shippers, carriers, and receivers also contributes to delayed recognition and inconsistent response efforts.

It can also be difficult to determine the value of lost merchandise because of differing inventory accounting practices. The expected retail price of an item is different than the cost and at various points in the supply chain, cargo owners may account via different measures, including how the items are accounted for by a third-party carrier or an insurance company. Furthermore, the loss in an accounting ledger or insurance claim may fail to reflect the full impact on a retailer, and rarely consider including reputational damage, operational disruption, the cost of replacing stolen goods, increased insurance premiums, and the loss of additional sales when consumers opt not to visit a retailer at all because of the inability to purchase the stolen item.

Cargo theft reporting practices also vary widely. Depending on the theft, the location, the parties involved, and many other factors, incidents may be reported only to local law enforcement, logistics providers' law enforcement or asset protection teams (e.g. rail police), third-party aggregators, insurance companies, or combinations of these. Members expressed concern about the lack of centralized or aggregated federal data.

Members agreed that DOT could play a meaningful role in improving response capabilities. Suggestions included aggregating police reports to create a national dataset, promoting standardized incident reporting, and investing in linked data systems such as weigh stations, license plate recognition (LPR) cameras, and Global Positioning System (GPS) tracking. Greater reporting and tracking of MC number misuse and bad actors is another opportunity. Additional infrastructure such as closed-circuit television (CCTV) surveillance and radio-frequency identification (RFID) technology was also recommended to support real-time detection and deterrence. These improvements would help close existing gaps and strengthen the overall resilience of the freight network against theft.

Law Enforcement Coordination

RILA members identified several challenges and opportunities for improving coordination among federal, state, and local law enforcement agencies. A recurring theme was the absence of a centralized repository for contacts and theft event data, including reports of misused MC numbers and identified bad actors. While many agencies may have jurisdiction over or interest in supply chain crime, there is a significant gap in how information is disseminated and shared across all parties

Greater law enforcement involvement in regional cargo security councils and international groups like TAPA³ (Transported Asset Protection Association) would help promote leading practices and foster collaboration. It could also encourage more investment in cargo theft task forces, better interdepartmental communication, and more consistent monitoring of known theft hotspots.

Retailers also report confusion and inefficiencies in the reporting process. In many cases, it is unclear whether to contact local, county, or federal authorities, which delays response times and lowers the chances of recovering stolen freight. Suggestions included the creation of a dedicated task force at the state or federal level, improved access to theft data (such as adding incident counts to carrier profiles on the SAFER⁴ system), and stronger protection for whistleblowers who may have knowledge of fraudulent or criminal activity.

These recommendations align with CORCA's goal of enhancing multi-jurisdictional coordination and improving the flow of actionable intelligence between law enforcement and private stakeholders.

Role of Federal Intelligence Functions

Retailers agree that federal intelligence agencies have an important role to play in identifying and mitigating cargo theft risks. Supply chain crime should be treated as a threat to the U.S. economy, regardless of the perceived severity of individual offenses. Retailers recommend that federal intelligence functions adopt a model similar to other crime categories, where broad networks of information exchange are actively managed and encouraged. Furthermore, the transnational nature of organized cargo theft networks (and indeed, of supply chains themselves) necessitates the involvement and participation of multiple U.S. government agencies.

To be effective, federal intelligence should proactively share offender information with the appropriate law enforcement agencies to support earlier intervention and investigation. Additionally, federal agencies consider administrative actions, such as removing DOT or

³ Transported Asset Protection Association. (n.d.). Cargo Crime Monitor. <https://database.tapa-global.org/cargo-crime-monitor/index>

⁴ Federal Motor Carrier Safety Administration. (n.d.). *Safety and Fitness Electronic Records (SAFER) System*. U.S. Department of Transportation. <https://safer.fmcsa.dot.gov/>

Standard Carrier Alpha Codes (SCAC) associated with fraudulent carriers, as part of a broader strategy to disrupt organized theft operations.

CORCA supports this approach by enabling federal agencies to proactively track and respond to organized crime networks, including those involved in cargo theft. Its framework encourages earlier intervention and administrative disruption of fraudulent actors.

Role of DOT Operating Administrations

The U.S. Department of Transportation's Operating Administrations — including the Federal Motor Carrier Safety Administration (FMCSA), Federal Highway Administration (FHWA), Federal Railroad Administration (FRA), Maritime Administration (MARAD), Federal Aviation Administration (FAA), and Pipeline and Hazardous Materials Safety Administration (PHMSA) — can play a meaningful role in addressing cargo theft by focusing on mode-specific vulnerabilities and improving coordination across agencies. Each administration has unique visibility into different segments of the supply chain, and their contributions should complement, rather than duplicate, the enforcement roles of the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS).

For example, FMCSA could enhance carrier vetting and oversight by improving the accuracy and transparency of carrier data, including flagging carriers with repeated theft incidents or fraudulent activity. FMCSA has already made strides in modernizing the tracking and vetting connected with MC numbers, and opportunities remain for greater transparency and monitoring of the use (or misuse) and transfer of numbers.

FRA and MARAD could support infrastructure improvements at rail yards and marine terminals, where theft often occurs due to limited surveillance and access control. The FAA could explore security protocols for high-value airborne freight, while PHMSA could assess risks related to hazardous materials theft.

Retailers encourage DOT to strengthen coordination across federal, state, and local agencies by establishing clear protocols for information sharing, joint task forces, and standardized reporting procedures. These efforts should be developed in close collaboration with industry stakeholders to ensure they are practical, scalable, and aligned with existing operations. DOT's operating administrations can further enhance their mode-specific initiatives by aligning with the broader enforcement strategy outlined in CORCA, helping to ensure cargo theft is addressed as part of a unified federal response to organized criminal activity.

Data Collection Improvements

Retailers strongly support efforts to improve cargo theft visibility through enhanced data collection. Current reporting is fragmented and inconsistent, making it difficult to assess the full scope of the problem. DOT could address this by developing a centralized reporting platform that

integrates data from FMCSA inspections, CBP systems, federal and other law enforcement entities, and third-party aggregators like CargoNet.

Such a platform should allow for timely reporting, standardized incident categorization, and secure data sharing between public and private entities. Retailers also recommend that DOT explore partnerships with insurance providers and logistics platforms to capture theft-related claims and operational disruptions. Improved data visibility would support better risk assessment, enforcement targeting, and policy development.

Regulatory Vulnerabilities

Certain regulatory gaps may inadvertently contribute to cargo theft vulnerabilities. For example, the ease with which parties can obtain or transfer MC numbers creates opportunities for fraudulent actors to re-enter the system under new identities. Additionally, the lack of mandatory vetting standards for brokers and carriers on load boards allows bad actors to exploit weak oversight.

DOT should continue to review existing regulations to identify areas where authentication, transparency, and accountability can be strengthened, and support FMCSA's ongoing work to fortify carrier registration practices. This could include more enhanced identity verification for carriers and brokers, real-time confirmation of carrier/driver legitimacy, mandatory reporting of theft incidents, and penalties for repeated violations. Addressing these regulatory gaps would help close loopholes that organized theft networks currently exploit.

Industry Best Practices and Technologies

Retailers have adopted a wide range of leading practices and technologies to reduce both opportunistic and organized cargo theft, with strategies tailored to the type of goods being shipped, the transportation mode, and the level of risk associated with specific lanes or facilities. It is important to note that soaring cargo theft has required retailers to devote significant time and investment to prevention, mitigation, post-event follow-up, and other efforts — adding additional operational costs to supply chains.

First and foremost, retailers have focused on establishing trusted networks of vendors, providers, and carrier partners, treating “know your partner” as a cardinal rule of supply chains. In many cases this has resulted in retailers working with fewer partners, conducting more frequent and more intensive carrier/partner vetting, instituting additional process checks, and tightening contract language and terms to increase security standards and protection requirements. Carrier and broker compliance is a cornerstone of retail freight security. Retailers have developed detailed security requirements for transportation partners, including:

- Carrier vetting and qualification
- Real-time vehicle tracking

- Use of tamper-evident seals
- Secure parking and route planning

For brokered freight, retailers have implemented third-party carrier requirements that define minimum security standards for subcontracted carriers (or limiting the use of subcontracting). Related policies include prohibiting the use of double-brokering, load boards, and other means of potential risk exposure. Additionally, some have partnered with carrier vetting platforms that enable comprehensive risk assessments and prequalification, ensuring only approved partners handle sensitive shipments.

Retailers also leverage contract language to hold carriers and brokers liable for cargo loss or damage, reinforcing accountability throughout the transportation process. For rail freight, in some cases retailers may negotiate for or pay a premium to have their containers placed on the bottom of a double-stack well car, where it is more difficult to gain unauthorized access.

In addition to leading practices for engaging with carriers and other logistics service providers, many retailers have undertaken basic physical infrastructure improvements at distribution centers and yards, including more/better camera coverage, improved fencing, and license plate and other camera-aided tracking systems. While physically hardening their facilities, retailers have also instituted stricter procedures for drivers to enter yards and pick up loads, including real-time identity verification, confirmation with carriers, documentation review (sometimes computer- or AI-enabled), shipment/carton audits, and more.

Technology also plays a key role in prevention and mitigation efforts. Many members with high-value, high-target shipments use electronic seals, open-door monitors, GPS tracking, in-truck cameras, and other technologies, especially for full truckload (FTL) shipments, where the risk of complete load loss is highest. It is important to understand that while GPS tracking remains a critical tool for locating stolen shipments, it is also one of the easiest technologies for bad actors to defeat. Therefore, GPS is most effective when paired with rapid law enforcement responses and integrated into broader security protocols.

Retailers handling very high-value or unique designer merchandise have implemented comprehensive security protocols across their supply chains. These may include:

- Packaging and labeling controls, such as concealed palletization and non-descriptive shipping labels, to reduce visibility of branded goods.
- Advanced vehicle technology, including GPS tracking with automated alerts for route deviations, forward and driver-facing cameras that activate upon ignition and continue recording post-shutdown, cargo-view cameras inside trailers, and cargo door sensors that log each opening and closing event with location data.

- Seal requirements—such as Customs Trade Partnership Against Terrorism (CTPAT)⁵ - certified ISO 17712 bolt seals—are critical for deterring tampering and ensuring shipment integrity.

At the facility level, inbound designer shipments undergo 100% carton audits to detect tampering or loss. Retailers also enforce secure parking protocols and require carriers to follow strict check-in procedures, including verification of up to 12 data points (e.g., truck number, trailer number, driver name, license number) before allowing access to pickup locations.

Industry collaboration plays a vital role in preventing theft. Retailers actively participate in organizations such as TAPA, which provides global security standards for trucking, facilities, and freight brokerage. Members share intelligence on theft trends, active investigations, and mitigation strategies with other shippers, transportation providers, and law enforcement agencies. This collaboration is especially valuable when organized retail crime investigations reveal shared threats or repeat offenders.

Ongoing education and engagement are key to staying ahead of evolving theft tactics. Retailers regularly attend cargo and retail theft conferences to monitor geographic risk areas, emerging methodologies, and technological advancements. These insights inform strategy and help refine security measures.

Finally, retailers are committed to building a culture of security across their organizations. Recognizing that theft prevention requires participation at every level; they invest in training, awareness campaigns, and internal accountability to empower employees to actively protect company assets—both in-store and in transit.

Measuring Success in Reducing Cargo Theft

Retailers recommend that DOT measure success by using frequency of incidents and dollar value of losses (using an agreed-upon standard definition) as primary reporting metrics. These two indicators provide a clear picture of both the scale and economic impact of cargo theft. The establishment of a centralized clearinghouse for reporting would be a critical first step, as no single accurate reporting point currently exists.

In addition to these core metrics, retailers suggest several other performance indicators that would help refine tracking and guide targeted interventions:

- Type of theft/fraud, including details and methodology, to track increasing/decreasing frequency of particular categories/tactics.
- Recovery rates to assess the effectiveness of law enforcement and investigative efforts.

⁵ U.S. Customs and Border Protection. (n.d.). *Customs Trade Partnership Against Terrorism (CTPAT)*. U.S. Department of Homeland Security. <https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT>

- Time-to-report, measuring how quickly incidents are communicated to authorities.
- Geographic concentration of thefts, identifying high-risk locations, corridors, and facilities.
- Mode-specific data, distinguishing between thefts in trucking, rail, air, and marine environments.
- Repeat offender tracking, to monitor patterns and support intelligence-led enforcement.
- Industry reporting participation rates, to evaluate the reach and adoption of reporting platforms.
- Bad actors identified by FMCSA's extended vetting/verification efforts for MC registration

Retailers also recommend tracking response times and resolution outcomes, such as arrests, prosecutions, or restitution, to better understand the end-to-end effectiveness of cargo theft mitigation efforts. These metrics would not only help measure progress but also inform future policy, infrastructure investment, and public-private collaboration.

Incorporating CORCA's framework into DOT's performance metrics, such as recovery rates, geographic targeting, and repeat offender tracking, would help ensure alignment with national efforts to combat organized retail crime.

Reporting Practices and Barriers

Retailers currently report cargo theft incidents to a mix of local law enforcement and specialized entities such as rail police and CargoNet. However, there is no unified federal system aggregating these reports, which limits visibility into the full scope of the problem. Reporting is often partial and inconsistent, and because multiple parties and locations may be involved, it may be unclear which companies are impacted or are responsible for reporting.

Clearer guidance on how and where to report thefts, especially at the federal level, would improve consistency and ensure that incidents are captured in national datasets. Retailers expressed interest in having a direct federal reporting pathway, in addition to local channels, to streamline the process and support more accurate data collection.

CORCA's emphasis on federal coordination and data sharing could help establish a unified reporting system, reducing fragmentation and improving visibility into cargo theft trends.

Forward-Looking: Innovative Practices and Technologies

Retailers believe that DOT has a unique opportunity going forward to pilot innovative approaches to cargo theft prevention, reporting, and enforcement partnerships. One of the most important lessons learned in recent years is that bad actors exist across all segments of the supply chain, including among merchandise vendors, logistics providers, and internal operations. These

actors often coordinate more effectively than legitimate stakeholders and are highly attuned to supply chain vulnerabilities. Rapid identification of these networks and their tactics would significantly improve prevention and enforcement efforts.

To support this, DOT could explore technologies such as AI-driven monitoring, exception reporting and response, predictive analytics, and integrated threat detection platforms that combine shipment data with law enforcement intelligence. Pilot programs focused on secure parking infrastructure, electronic seals, and enhanced carrier authentication could also yield valuable insights. Additionally, DOT could convene multi-stakeholder working groups to test new reporting protocols and data-sharing models.

Conclusion

Cargo theft remains a persistent and costly challenge for retailers—and the entire retail supply chain—with impacts that extend beyond financial loss to include operational disruption, consumer trust, and public safety. RILA members have implemented a wide range of leading practices and technologies to protect their goods in transit, but the scale and sophistication of organized theft networks demand a coordinated federal response.

DOT has a critical role to play in strengthening cargo theft prevention across transportation modes. By improving data collection, exercising oversight and vetting of carriers and logistics service providers, supporting law enforcement coordination, and investing in infrastructure and technology, DOT can help close existing gaps and reduce vulnerabilities. By aligning DOT's initiatives with CORCA's framework, federal agencies can more effectively disrupt organized theft networks, protect supply chain integrity, and enhance public-private collaboration.

RILA looks forward to continued collaboration with DOT and other federal partners to advance these priorities and safeguard the movement of goods across the country.

Sincerely,

A handwritten signature in black ink, appearing to read 'SG', with a long horizontal flourish extending to the right.

Sarah Gilmore
Senior Director, Government Affairs
Retail Industry Leaders Association (RILA)