Response to DOT RFI on Cargo Crime

Submitted by: National Motor Freight Traffic Association (NMFTA)
Date: 20 OCT 25

General (All Stakeholders)

Cargo theft remains one of the most persistent and evolving threats to the U.S. supply chain. NMFTA urges the Department of Transportation (DOT) to take decisive action to address both traditional and cyber-enabled cargo theft through coordinated, data-driven, and industry-supported initiatives.

Key Threats

- **Cyber-enabled diversion schemes** are now the leading method of strategic cargo theft, including fraudulent carriers, FMCSA account takeovers, and load board exploitation.
- **Insider collusion and credential theft** are increasingly used to bypass security protocols.
- **Telematics exploitation** allows criminals to track and reroute shipments in real time.
- **Straight thefts** of parked trucks and trailers remain prevalent, often aided by cyber reconnaissance.

Modal Risk Assessment

Truck and multimodal exchange points face the highest risk (rated 5/5), followed by rail (4/5), maritime (3/5), and air (2/5). Multimodal complexity and lack of unified oversight exacerbate vulnerabilities.

Barriers to Response

- Fragmented reporting systems and jurisdictional confusion.
- Industry reluctance to report due to reputational concerns.
- Lack of real-time data sharing and centralized intelligence.

1: What are the most significant cargo theft risks facing the U.S. supply chain today?

- **Strategic cargo theft networks** Strategic cargo theft networks increasingly leverage cyber-enabled diversion schemes, including FMCSA account takeovers and load board exploitation.
- **Insider collusion**, often combined with credential theft or social engineering.
- **Identity theft of carriers/brokers**, allowing criminals to fraudulently obtain freight tenders.
- **Telematics exploitation**, where unsecured or outdated fleet management systems are manipulated to track or reroute shipments.
- **Straight thefts** Traditional straight thefts remain significant but are now often supported by cyber reconnaissance.
- **Complexity of Cargo Theft**, as described by the NMFTA Cyber-enabled Cargo Theft Reduction framework.

2: How do these risks vary across different types of goods movement?

- **Truck-borne freight:** Most at risk from cyber-enabled theft, fraudulent carriers, telematics exploitation, and straight theft.
- **Rail:** Pilferage at yards, switch locations, holding areas, and intermodal terminals, sometimes coordinated with insider knowledge. Blindspot for slow moving trains and lack of Federally funded Rail police, or cooperations with Local LE.
- **Maritime:** High-volume risk at marine terminals and during vessel-truck-rail transfers, particularly with containers targeted for identity fraud and document manipulation.
- **Air:** Opportunistic theft in cargo-handling areas, often insider-assisted.
- **Multimodal exchanges:** Most vulnerable to fraudulent diversion and cyber-enabled identity-based schemes due to complex handoffs.

3: Challenge rating (1–5) per mode of transportation:

- Truck: **5**
- Rail: 4
- Waterborne (maritime): 3
- Air: **2**
- Multimodal exchange points: **5**

4: What barriers prevent timely detection, reporting, and response to cargo theft incidents?

- **Fragmented reporting** Fragmented reporting channels across agencies and industry hinder timely response.
- **Fear of reputational harm**, deterring carriers/brokers from reporting.
- **Unclear jurisdiction** between DOT, DHS, FBI, TSA, CISA, other DOJ LE, and state/local authorities.
- **Lack of real-time data sharing platforms** to support lateral and vertical communication.

Recommendation: NMFTA proposes an anonymized threat information sharing hub for reporting cyber-enabled cargo crime, with optional attribution, propagating data to government and industry to improve visibility and trends analysis. NMFTA proposes one of three protentional solutions:

1. Use an existing Watch Center or Intelligence Operations Center as a central point of reporting.
2. Support and Fund an NMFTA Fusion Center that facilitates intelligence Sharing within the transportation industry as well as centralized anonymous Cargo theft reporting that can be disseminated outward as required. This should include JTF-cargo theft interaction with Local, State, Federal LE, and State trucking associations.
3. DOT support the passing House Bill H.R.2853 - DOT should support passage of H.R.2853 and establish a cargo theft reporting portal integrated with a threat intelligence center.

Law Enforcement / Security

5: How can law enforcement better coordinate?

- Expand existing FBI JTF and HSI “Operation Boiling Point” task forces with greater DOT participation, with clear delineation with JTF Lead, and support and supporting roles.
- Establish clear referral pathways for initial cargo crime reports to avoid jurisdictional confusion.
- Support information sharing between federal and state/local task forces through DOT-facilitated reporting platforms.

6: What role should Federal intelligence functions play?

- Provide strategic analysis of organized cargo theft rings and dissemination of threat intelligence to industry.
- Correlate cyber intrusion indicators with physical theft events for early warning.
- Integrate cargo theft into existing DHS/CISA and FBI intelligence products.

DOT Operating Administrations / Federal Agencies

7: How should DOT Operating Administrations contribute?

- FMCSA: Improve security of carrier/broker authority issuance (e.g., Real ID or biometric verification to prevent fraudulent entities).
- FHWA: Support secure parking initiatives to reduce straight theft opportunities.
- FRA & MARAD: Coordinate on rail/maritime incident reporting into shared systems.
- FAA & PHMSA: Ensure dangerous goods movements incorporate cargo theft risk assessments.
- DOT agencies should coordinate to avoid duplication of FBI/DHS investigations, focusing instead on prevention, reporting infrastructure, and resilience.

8: What data collection improvements should DOT pursue?

- Develop a centralized, multi-modal cargo theft reporting system, integrated with FMCSA inspections and CBP trade data.
- Ensure data is structured for intelligence analysis (incident type, method, commodity, location, loss value).
- Enable industry anonymized submissions via NMFTA's proposed reporting hub.

9: Are there regulations that cause/contribute to vulnerabilities?

FMCSA authority issuance process can be exploited by criminal entities posing as carriers/brokers. Stronger identity verification is needed.

Industry Stakeholders

10: What industry best practices or technologies are effective?

- GPS tracking & electronic seals for load visibility.
- AI-driven monitoring & anomaly detection in TMS and telematics.
- Secure parking initiatives (fenced, monitored, access-controlled).
- Cybersecurity frameworks (e.g., NMFTA's Cybersecurity Best Practices for Mid-Sized Fleets, 2025) aligned with NIST CSF 2.0.
- DOT sponsored program to ensure validation testing of all telematics and ELD devices to ensure cyber resiliency

Recommendation: Propose NMFTA stand up a Certification program in conjunction with and supported by DOT to ensure that carriers and brokers have an acceptable level of minimal Cybersecurity maturity

Combine this approach with the current work that NMFTA is Doing with NIST NCCoE to build a Transportation Industry specific Community Profile for Cybersecurity.

11: How should DOT measure success?

- Reduction in successful thefts (both straight and strategic).
- Increased incident reporting rates into centralized systems.
- Time-to-detection and time-to-recovery metrics for stolen cargo.
- Growth of public-private information sharing participation.
- The Number of Carriers brokers “audited” to a minimal level for Cybersecurity.

12: To what agency/jurisdiction does industry report theft? Barriers?

- There are no clear and published Guidelines or reporting structures in place.
- Current reporting: Local police, state police, FBI JTF, NICB, and insurers.
- Barriers: Lack of clarity on federal reporting, inconsistent response times, concern over confidentiality.
- Recommendation: DOT should sponsor a single-entry reporting portal that routes incidents to correct agencies, with anonymization options.
- Clear reporting methodologies with a focus on disruption of criminal activities from point of theft, joint operations between local, state and federal agencies

13: Which commodities face the highest risks?

- Non-serialized consumables: Energy drinks, food, alcohol, and tobacco.
- Pharmaceuticals, electronics and other traceable but high-value commodities.
- Export containers and shipments near ports are disproportionately targeted due to high resale value.
- Domestic vs. imported/exported: Imported/exported goods at ports face greater risk due to organized international crime networks and intermodal complexities
- Raw building materials.
- Any commodities that can be cross-docked and sold at speed of retail

Forward-Looking

14: What potential practices or technologies should DOT initiate?

- Pilot an industry-government cargo crime information sharing portal (built in partnership with NMFTA and industry carriers).
- Explore AI-based anomaly detection in freight documentation to identify fraudulent carriers/diversions.
- Expand secure parking networks funded through DOT infrastructure programs.
- Conduct multi-modal tabletop exercises with industry, DHS, TSA, Local, State and Federal LE, and DOT to simulate coordinated cargo theft responses.

Summary of Key NMFTA Positions:

1. **Centralized Reporting Platform**: DOT should sponsor a single-entry, anonymized cargo theft reporting portal integrated with NMFTA's proposed hub. As proposed in the recommendations to question number four.
2. **Cybersecurity Certification Program**: Support NMFTA in establishing a DOT-backed certification for carriers and brokers to ensure minimum cybersecurity maturity. Putting the primary focus of NIST in conjunction with partners working to build and shape a community profile for the transportation industry.
3. **Secure Parking Expansion**: Fund infrastructure projects to reduce theft opportunities at rest stops and terminals.
4. **Identity Verification Reform**: FMCSA should implement biometric, Real ID or other like type systems that allow for verification to prevent fraudulent carrier/broker registrations.
5. **Public-Private Intelligence Sharing**: Expand FBI JTF and HSI task forces with DOT participation and support joint operations with local/state LE. Places an emphasis on collaborative frameworks (TSA, HSI, CISA, FBI JTF) to align with DOT's coordination role.
6. **Data-Driven Metrics**: Measure success via reduction in thefts, improved detection/recovery times, and increased reporting rates.
7. **Awareness Campaigns**: Launch a cargo theft "Eagle Eyes" program with clear reporting protocols and industry-wide PSAs.

Call to Action

Cargo theft is no longer just a physical crime — it is a cyber-physical threat that undermines national commerce, public safety, and economic resilience. DOT must act now to unify reporting, strengthen cybersecurity across the transportation sector, and empower industry stakeholders with the tools and intelligence needed to defend the supply chain.

NMFTA stands ready to partner with DOT to build a safer, smarter, and more secure freight ecosystem. The time for coordinated action is now.

Reference Documents

https://info.nmfta.org/cybersecurity-best-practices-guidebook-mid-sized-fleets

https://info.nmfta.org/nmfta-cybersecurity-cargo-crime-reduction-framework

https://nmfta.org/wp-content/media/2025/09/082525-R2R_Vendor_Risk-Framework-1.pdf