DEPARTMENT OF WAR

SURFACE FREIGHT SECURITY ASSESSMENT

A Comprehensive Investigative Report on Systemic Vulnerabilities in American Commercial Motor Vehicle Transportation and Their Implications for Military Surface Freight, Federal Logistics, and National Security

Prepared by

Rob Carpenter, CDS., CDM/E

Chief Intelligence Officer, Tea Technologies, Inc.
VP of Compliance, TruckSafe Consulting

May 2026

Prepared in conjunction with the NDTA-CAS Surface Force Projection Meeting
Christopher Newport University | Newport News, Virginia | May 18-21, 2026

Table of Contents

I. EXECUTIVE SUMMARY

The United States military moves billions of dollars in freight across American highways every year through the same commercial motor vehicle network that is currently compromised at nearly every level of regulatory oversight, driver credentialing, carrier vetting, vehicle integrity, and financial responsibility. This assessment documents, with data derived from Tea Technologies' analysis of 8,183,916 roadside inspections and 5,144,926 crash records, the systemic vulnerabilities in American surface transportation that directly threaten the security and integrity of the Department of War freight. The central finding of this assessment is that carriers hauling government freight are failing at rates dramatically above the national average, and that pure DOD and military freight is in substantially worse condition than even the broader government freight universe. Across 29,030 confirmed government freight inspections in Tea Technologies's database, involving 7,451 distinct carriers, the aggregate out-of-service rate is 17.71 percent. When the data is filtered to pure DOD and military freight only, the OOS rate climbs to 20.55 percent across 5,879 inspections involving 3,624 distinct carriers. When FMCSA-certified inspectors conduct a full Level I 37-step inspection on DOD freight vehicles, 30.93 percent are placed out of service. The Level I OOS rate across all government freight reaches 32.24 percent. One in three trucks fails a real inspection. The national vehicle OOS rate from the 2025 CVSA International Roadcheck was 18.1 percent. Government freight carriers are failing at rates that exceed the national benchmark by significant margins across every measurement cohort.

The data reveals a subcontracting chain so fragmented that it defies any claim of managed-carrier oversight. The shipper name "US ARMY" appears with 251 different carriers across 306 inspections. "US MILITARY" shows 173 different carriers. "US NAVY" shows 73. The SDDC 841st Transportation Battalion, responsible for coordinating military freight through the Charleston Strategic Seaport, produced a 100 percent OOS rate across 11 inspections. Red River Army Depot produced 47.6 percent. Oshkosh Defense produced 43.2 percent. The quarterly trend is deteriorating OOS rates on government freight have been climbing since mid-2023.

This assessment expands the analysis beyond DOD to document carrier risk across 13 federal agency portfolios, including the Department of Homeland Security, Department of Energy, USDA, NASA, Department of Justice, Treasury, Health and Human Services, Department of the Interior, GSA, VA, and state and local governments. Among confirmed categories, USDA and Forest Service carriers exhibit the worst Level I OOS rate at 53.0 percent. DOE and nuclear-complex carriers run a 38.8 percent Level I OOS rate. USPS contractors show 35.2 percent. NASA aerospace freight carriers show 24.8 percent. The federal freight ecosystem is failing across every agency.

The broader trucking ecosystem through which this freight moves is under assault from converging threat vectors. CDL fraud pipelines have produced 6,000+ fraudulent licenses linked to 13 deaths. A wanted jihadist recruiter obtained a Pennsylvania CDL and was driving commercially when ICE arrested him. Medical examiner fraud mills invalidated 6,000 driver certifications in a single takedown. SAP fraud has undermined the Drug and Alcohol Clearinghouse. ELD manipulation runs on a self-certification model with no government testing. Chameleon carriers exposed on CBS's 60 Minutes cycle through identities faster than enforcement can act. Chinese state interests have penetrated American port infrastructure, farmland, rail supply chains, and logistics visibility platforms. The FBI published a Public Service Announcement on April 30, 2026 warning that cyber-enabled strategic cargo theft surged to $725 million in 2025, a 60 percent increase. The Supreme Court ruled 9-0 on May 14, 2026 that freight

brokers are liable for carrier selection, implicating the same brokerage system that dispatches DOW freight. The convergence of these threats is not coincidental. It is systemic.

The crash exposure data for the government freight carrier portfolio is staggering. Carriers confirmed to have participated in federal freight movement were involved in 211,888 crashes over a 24-month period, including 5,381 fatal crashes resulting in 6,102 fatalities. The DHS portfolio alone accounts for 21,014 crashes, 539 fatal, 563 fatalities. These are not crashes that occurred while hauling government freight. The crash datasets do not identify shipper attribution at crash time. But these are the carriers that the government is hiring to move its freight, and their collective safety record represents a portfolio of risk that no private-sector logistics operation would accept.

Cargo integrity findings across the government freight carrier portfolio identify 5,029 cargo-integrity violations, 3,099 of which resulted in out-of-service orders, a 61.6 percent OOS conversion rate. Among these, 1,238 general cargo securement violations converted at 87.6 percent OOS. Intermodal container securement violations converted at 97.2 percent OOS. Hazmat placard and securement violations totaled 1,116 events. Shifting and falling cargo produced 737 events at 69.1 percent OOS. Government property is being transported on vehicles with inadequate securement, and the OOS conversion rates indicate that when inspectors find these conditions, the deficiencies are severe enough to require immediate remediation in the overwhelming majority of cases.

Among individually scored DOD carriers, 156 crashes were recorded over 24 months, including 11 fatal crashes resulting in 15 fatalities. Three carriers carry chameleon flags. Five are insured by HIGH RISK-rated insurers. Six controlled substance and alcohol violations were identified on DOD carriers, every one resulting in an out-of-service order. Drivers hauling for the Department of Defense and Total Military Management were caught with narcotics and amphetamines in the cab, four times in eighteen months at one carrier alone.

Foreign-domiciled carriers appear in the military freight data. Mexican carriers haul Titan Marine Fuel and Tododren cargo with OOS rates exceeding 100 percent. Canadian carriers haul loads designated “Canadian Military” and “Canadian National Defense” through Alaska. The non-domiciled CDL pathway that allowed a Chinese national to kill an American trucker on I-40 and an Uzbek terrorist to drive commercially remains open. There is no systematic screening of DOW freight carriers against the Section 1260H Chinese Military Companies list. This prohibition does not take full effect for direct procurement until June 2026, and for indirect procurement until June 2027.

This assessment is not a theoretical risk analysis. It is not a compliance review. It is not a policy proposal. It is a documented, data-driven, investigative intelligence product describing what is happening right now on American highways with Department of War freight, federal civilian freight, and the commercial motor vehicle network on which both depend.

In the language of the Irregular Warfare Center’s contested logistics framework: freight execution is no longer a benign administrative function. It is part of the operational kill chain, contested persistently and often invisibly.

II. STRATEGIC CONTEXT: FREIGHT EXECUTION AS CONTESTED TERRAIN

The core strategic question facing the United States surface transportation enterprise is whether the nation can assure trusted freight movement in a contested environment. The NDTA Surface Force Projection Meeting breakout session on "Freight Management in the Contested Environment," convened by MG (Ret.) Edward Dorman of the Irregular Warfare Center, frames this question through three lenses that structure this entire assessment.

Threat

State and non-state actors increasingly exploit commercial freight transportation networks using non-kinetic means. Shell companies, illicit brokerage practices including double and triple brokering, compromised licensing regimes, cyber intrusion, and data manipulation allow adversaries to gain access to, visibility into, or influence over cargo movements without triggering traditional security thresholds. The continued lack of identification of and continued award of tenders to illicit carriers who are seemingly legitimately registered undercuts legitimate carriers' profit margins and begins to drive them away from supporting the national defense transportation carrier base. Additionally, these allow adversaries to gain access to, visibility into, or influence DOD cargo movements while also threatening safety in the homeland due to an inability to comprehensively audit driver certification and equipment usage.

Documented industry reporting demonstrates recurring cases where carriers with insufficient physical capacity, lapsed or revoked authorities, or prior fraudulent behavior continue to access DOD freight through opaque award and execution pathways. Static or episodic vetting mechanisms are insufficient against adaptive threats operating continuously.

Environment

The freight ecosystem is commercially dominated, fragmented across authorities and systems, data-disconnected, operationally complex, and increasingly stressed by market distortion and criminal exploitation. No single organization currently possesses complete visibility or authorities across the freight ecosystem. ARTRANS operates within a transportation environment defined by heavy reliance on commercial capacity, fragmented and non-integrated data systems, regulatory complexity across federal, state, and commercial domains, volatile market conditions, and risk to homeland security as underqualified carriers move hazardous and oversize cargo at risk to infrastructure and safety within the United States.

Current assumptions place significant reliance on Transportation Officers at the point of loading to mitigate risk. However, real-world conditions, including the training and certification of both military and civilian TO workforce, time-sensitive shipments, fixed port sail dates, distributed execution, and limited on-site presence frequently render this approach impractical. The environment routinely places TOs in no-win situations: delay mission-critical cargo or accept execution risk due to insufficient real-time visibility and verification or alternative lift provision. This is not a failure of diligence or training. It is a mismatch between system design and operational reality.

Self

Many current systems, processes, and governance structures were designed for permissive environments, periodic compliance validation, fragmented oversight, and administrative throughput. The current environment requires continuous validation, integrated visibility, resilience-focused oversight, trusted carrier ecosystems, and faster policy adaptation. The environment evolved faster than the governance architecture.

Internal processes, policies, authorities, and governance structures compound risk. Current approaches emphasize periodic compliance checks rather than continuous validation, manual enforcement rather than automated detection and analytics, distributed responsibility without centralized end-to-end accountability, and failure to access cross-enterprise domain data. This has led to an institutional posture optimized for efficiency and throughput in a permissive environment, rather than resilience and control in a contested one. Procedural compliance is often conflated with operational assurance, masking systemic vulnerability.

What appears as isolated fraud, safety violations, or compliance drift is, in aggregate, a market-shaping dynamic that mirrors adversary economic warfare strategies: eroding trust, displacing legitimate capacity, and increasing systemic risk to the Department.

The May 13, 2026 coordination meeting between MG (Ret.) Dorman, Rob Carpenter, Don Welchoff, COL Steven Putthoff (Deputy, ARTRANS), Jeff Olenick (GFM Program Manager, ARTRANS), and Cody Honeycutt (US Bank/former USTRANSCOM J9) reinforced broad consensus that the issues emerging within the Defense Transportation System represent a larger contested freight ecosystem challenge requiring continued collaboration across government, industry, and interagency partners. No single organization possesses sufficient visibility, authority, or capability to address the issue independently.

III. METHODOLOGY, DATA SOURCES, AND ANALYTICAL FRAMEWORK

Tea Technologies Platform and Scoring

This assessment was produced by Tea Technologies, Inc., operator of the Tea Technologies Highway Intelligence platform (theteaintel.com), using proprietary carrier scoring algorithms, 30+ FMCSA API integrations, and integrated inspection and crash databases. Tea Technologies holds provisional patent Application No. 64/009,415 (filed March 18, 2026). The Tea Technologies carrier score is a 0-to-100 numeric risk score calculated from crash history, out-of-service rates, violation patterns, authority revocation history, authority age, and insurer quality.

Primary Datasets

The inspection dataset comprises 8,183,916 roadside inspection records from February 2023 through January 2026 (36 months). Each record includes 30 fields: carrier identification and domicile (city, state, zip), shipper name, inspection date and location (state, county, description), inspection level, violation counts by category (driver, vehicle, hazmat), OOS determinations by category, post-accident indicator,

hazmat placard requirement, cargo tank indicator, and gross combined vehicle weight. The crash dataset contains 5,144,926 records from January 1982 through May 2026.

The FMCSA violations database contains 2,417,522 individual violation records with CFR violation codes, BASIC categories, severity weights, OOS indicators, and unit citation counts. The MCMIS census data covers all registered motor carriers with authority status, power unit counts, driver counts, mileage, and domicile information. Insurance data includes insurer names, policy amounts, and coverage types for the carrier universe.

Government Freight Identification Methodology

Government freight inspections were identified through a multi-layer shipper name taxonomy. The full government freight universe totals 29,030 confirmed inspections across 7,451 distinct carriers. The pure DOD/military subset totals 5,879 inspections across 3,624 carriers. Thirteen federal agency categories are profiled: DOD, DHS, USPS, DOE, USDA, DOJ, Treasury, HHS, DOI, GSA, NASA, VA, and State/Local.

Crash attribution carries an important caveat: the FMCSA crash system does not identify whether a crash occurred while hauling federal freight. The crash data identifies carriers confirmed to have participated in federal freight movement; their crash record represents portfolio-level risk exposure, not load-specific attribution.

Comparative Benchmarks

National benchmarks are derived from CVSA's 2025 International Roadcheck (56,178 inspections): vehicle OOS rate 18.1 percent, driver OOS rate 5.9 percent. Brake systems account for 40+ percent of vehicle OOS. Tires account for 21.4 percent. False records of duty status were the second-most-cited driver violation in 2025, with 58,382 total. The 2026 Roadcheck Day 1 data showed a 31.4 percent OOS rate across 1,580 inspections.

IV. THE DEFENSE FREIGHT TRANSPORTATION SERVICES CONTRACT

The Defense Freight Transportation Services contract is the primary mechanism through which USTRANSCOM procures surface freight transportation for the Department of War. DFTS I was awarded to Crowley Logistics in November 2016 for $2.23 billion. The first cargo moved from Tobyhanna Army Depot in Pennsylvania on February 12, 2018. In July 2024, USTRANSCOM awarded DFTS II to Crowley, another $2.3 billion seven-year contract. During DFTS I, Crowley expanded its carrier network by more than 500 percent, growing from approximately 400 contracted carriers at launch to a network servicing 300,000 movements annually across 41 major depots and more than 500 destinations. More than $600 million in subcontracting went to small and diverse businesses.

The contract operates under a fixed-price agreement covering all lanes for each contract year. Crowley's TMS, built on 3Gtms technology deployed on Amazon Web Services, manages carrier selection, dispatch, tracking, and proof-of-delivery. When Crowley tenders a load to its carrier network, that

carrier may subcontract. The subcontractor may post on a load board. An owner-operator bids. The driver who arrives at a military depot may be four or five layers removed from Crowley, and neither Crowley nor USTRANSCOM may know who is behind the wheel.

The Defense Transportation Regulation, Part II, Chapter 205 establishes protective security requirements for DOD freight. Brokers, DFTS TSPs, sub-TSPs, freight forwarders, shipper agents, and shipper associations are explicitly restricted from handling Class 1 Divisions 1.1 through 1.6, sensitive munitions, arms, and shipments requiring Security Escort Vehicle Service, Protective Security Service, Dual Driver Protective Service, Constant Surveillance Service, and other high-security services. Canadian-based commercial drivers may transport goods from Canada to the United States if all goods were loaded in Canada and the Canadian companies have completed Level II (SECRET) facility and personnel security clearance requirements. Purely domestic service, point-to-point within the United States, is not permitted for Canadian TSPs.

The DTR requires Transportation Officers to conduct advance shipment planning, verify security clearances for personnel handling classified material, ensure DD Form 626 Motor Vehicle Inspection standards are met, and coordinate with installation security and force protection officers. The regulations exist. The data in this assessment demonstrates that compliance with these regulations is not being verified at the operational level. A $2.3 billion contract with 500 percent carrier expansion and 300,000 annual movements does not have the infrastructure to verify DTR compliance across its subcontracting chain.

GSA performed post-payment audits of DFTS I under the Transportation Act and issued notices of overcharge. Crowley disputed the interpretation. The contracting officer sided with Crowley but directed resolution through the Transportation Act process. Crowley sued in federal district court in August 2021. The litigation extended through 2023 and influenced the DFTS II solicitation. If payment mechanisms trigger multi-year federal litigation, what confidence is there that operational security mechanisms receive adequate attention?

The system is optimized for cost and throughput. It is not optimized for security. The DFTS contract expanded Crowley's carrier network by 500 percent. This assessment documents where that expansion leads.

V. THE STATE OF MILITARY SURFACE FREIGHT: FULL-SPECTRUM DATA ANALYSIS

The Verified Government Freight Universe

Metric	Value	National Benchmark	Delta
Total confirmed inspections	29,030	56,178 (2025 Roadcheck)	
Total unique carriers	7,451		
Total OOS events	5,141		

Metric	Value	National Benchmark	Delta
Government freight OOS rate	17.71%	18.1% (vehicle)	-2%
Level I inspections	6,020		
Level I OOS rate	32.24%	18.1%	+78%

Source: Tea Technologies, fed-v1 taxonomy, confirmed categories (Feb 2023-Jan 2026); CVSA 2025 Roadcheck

The all-inspection OOS rate of 17.71 percent for the government freight universe appears close to the national benchmark. This number is misleading. The aggregate rate is suppressed by the high volume of Level III driver-only inspections, which examine credentials and logs but never look at the vehicle. When inspectors conduct a full Level I, 37-step North American Standard Inspection on government freight vehicles, 32.24 percent are placed out of service. Nearly one in three. That rate is 78 percent above the national vehicle OOS benchmark.

Pure DOD/Military Freight

Metric	Value
Total DOD/military inspections	5,879
Total unique carriers	3,624
Total OOS events	1,208
Pure DOD/military OOS rate	20.55%
Level I inspections	1,426
Level I OOS rate	30.93%

Source: Tea Technologies, DOD/military shipper filter (excludes USPS, commercial false positives)

The 3,624 distinct carriers across 5,879 inspections means each carrier averages fewer than 1.63 inspections. This is not a managed fleet. This is a revolving door.

Government Freight by Category

Category	Inspections	Unique Carriers	OOS	OOS Rate	Level I OOS
DOD	1,424	857	307	21.56%	33.84%
Military Branch	1,268	926	260	20.50%	29.32%
Defense Logistics	561	421	121	21.57%	29.52%

Source: Tea Technologies, confirmed DOD subcategories

DOD-specific inspections produce a 33.84 percent Level I OOS rate, the highest among the military subcategories. More than one in three DOD trucks subjected to a full inspection is ordered off the road.

VI. PURE DOD/MILITARY FREIGHT: THE OOS CRISIS

Military Shipper OOS Rates: Installation by Installation

Shipper	Carriers	Inspections	OOS	OOS Rate	Violations
SDDC 841st Trans. Bn.	10	11	11	100.0%	76
Tododren SA de CV	13	17	19	111.8%	75
Dodson Valco	27	27	21	77.8%	98
Oshkosh Defense LLC	12	13	8	61.5%	51
US DOD	12	16	9	56.3%	44
Dodson	8	18	10	55.6%	56
Total Military Mgmt	5	11	6	54.5%	36
Red River Army Depot	19	21	10	47.6%	29
Tododren	8	13	6	46.2%	35
US MILITARY	173	199	89	44.7%	400
Oshkosh Defense	34	44	19	43.2%	90
MILITARY	82	97	40	41.2%	157
US Army Reserve CMD	27	29	11	37.9%	51
United States Army	14	17	6	35.3%	24
US Navy	73	81	28	34.6%	151
US Army Depot Sierra	14	15	5	33.3%	23
Department of Defense	39	62	20	32.3%	68
US Air Force	58	70	22	31.4%	76
US Army	251	306	71	23.2%	352

Source: Tea Technologies, military shipper analysis (excludes postal, commercial false positives)

The SDDC 841st Transportation Battalion, the Army's component responsible for managing military freight through the Charleston Strategic Seaport, produced a 100 percent OOS rate. Every single truck inspected on loads for the 841st was placed out of service, generating 76 violations across 11

inspections involving 10 different carriers. This unit coordinates force projection through one of DOD's designated Strategic Seaports.

Oshkosh Defense, the manufacturer of tactical military vehicles including the Joint Light Tactical Vehicle and the Family of Heavy Tactical Vehicles, shows a combined OOS picture that should alarm any logistics planner. Under its standard shipper name, 34 carriers across 44 inspections produced a 43.2 percent OOS rate. Under the "Oshkosh Defense LLC" variant, 12 carriers across 13 inspections produced 61.5 percent. The carriers moving Oshkosh military vehicles across American highways are failing at nearly triple the national vehicle OOS rate. These are the vehicles that equip the Army's combat brigades. They are being transported on trucks that cannot pass a roadside inspection.

Red River Army Depot, the Army's only remaining organic industrial base for wheeled vehicle and ground combat system repair, produced a 47.6 percent OOS rate across 21 inspections involving 19 different carriers. Nearly half the trucks hauling to or from the facility that maintains the Army's fighting vehicles are themselves mechanically unfit for the road.

Total Military Management, the entity that coordinates military household goods shipments for service members and their families during PCS relocations, shows a 54.5 percent OOS rate. More than half. The trucks moving military families' personal belongings are failing inspections at rates that would trigger immediate fleet suspension in any private-sector operation.

Tododren SA de CV, a Mexican-domiciled carrier (SA de CV is the Mexican corporate designation equivalent to a U.S. corporation), shows a 111.8 percent OOS rate across 17 inspections. An OOS rate exceeding 100 percent means that, on average, multiple OOS conditions were identified per inspection, both driver and vehicle OOS on the same stop. This carrier is hauling loads with military freight designations across the U.S.-Mexico border corridor with catastrophic safety performance. Thirteen different carriers appear under this shipper name, suggesting the same subcontracting fragmentation found in the domestic military freight data.

The 251 different carriers appearing under "US ARMY" alone are the most damning evidence of subcontracting fragmentation in this dataset. 306 inspections, 251 different carriers, 1.22 inspections per carrier. Nearly every carrier appears exactly once. There is no carrier continuity. There is no relationship-based oversight. There is no way to build a safety performance baseline for a carrier that hauls one Army load and disappears from the data.

VII. FEDERAL CIVILIAN FREIGHT EXPOSURE: CARRIER RISK ACROSS 13 AGENCY PORTFOLIOS

This section extends the analysis beyond DOD to the broader federal freight ecosystem. The federal government ships freight through commercial carriers across every cabinet department and independent agency. Each of these agencies relies on the same commercial carrier network documented in this assessment, and each faces the same systemic vulnerabilities.

Agency Portfolio Summary

Category	Inspections	Unique Carriers	OOS Rate	L1 OOS Rate	Status
USDA	414	323	31.9%	53.0%	CONFIRMED
DOE	672	379	21.0%	38.8%	CONFIRMED
USPS	740	432	19.2%	35.2%	CONFIRMED
VA	34	26	26.5%	–	CONFIRMED
NASA	117	94	24.8%	–	CONFIRMED
DOI	191	152	24.1%	39.4%	CONFIRMED
GSA	166	106	24.1%	23.1%	CONFIRMED
State/Local	2,617	1,331	17.4%	18.4%	CONFIRMED
DOD	3,923	2,611	19.7%	29.2%	PARTIAL
HHS	736	526	20.1%	31.1%	PARTIAL
DOJ	6,394	3,752	21.6%	30.3%	PARTIAL
DHS	86,190	35,157	22.3%	30.3%	NOT REPRODUCIBLE
Treasury	8,807	4,068	17.4%	26.7%	NOT REPRODUCIBLE

Source: Tea Technologies, fed-v1 taxonomy. DHS/Treasury/DOJ counts inflated by substring artifacts, requiring repopulation. Long-phrase categories confirmed.

USDA / Forest Service: The Worst Level I OOS Rate Among Federal Civilian Shippers

USDA and Forest Service carriers exhibit the worst Level I OOS rate of any confirmed federal civilian category: 53.0 percent. Of 83 Level I inspections conducted on carriers hauling for the Department of Agriculture and the Forest Service, 44 resulted in out-of-service orders. More than half of all USDA freight trucks fail a full inspection. The all-inspection OOS rate for USDA is 31.9 percent, roughly 1.7 times the Level I rate inversion expected when Level III inspections dilute the aggregate. USDA freight includes agricultural products, Forest Service equipment, and supplies moving to and from national forests, research stations, and rural installations. The carriers moving this freight are operating in some of the most remote and challenging terrain in the country, making mechanical failure not merely a compliance issue but an active safety hazard.

DOE/Nuclear Complex: High-Severity Exposure

DOE carriers serving the nuclear weapons complex, national laboratories, and energy facilities exhibit a 38.8 percent Level I OOS rate across 379 unique carriers. The facilities served include Los Alamos National Laboratory, Sandia, Oak Ridge, Savannah River, and the Pantex Plant. The cargo moving through these corridors includes radiological materials, precision instruments, classified components, and materials governed by the Atomic Energy Act. A 38.8 percent Level I OOS rate on vehicles serving

the nuclear enterprise represents a safety exposure that the National Nuclear Security Administration should find unacceptable.

USPS: The Postal Service Supply Chain

USPS contractors run a 35.2 percent Level I OOS rate across 145 Level I inspections involving 432 unique carriers. The Postal Service recently announced it will phase out contracted drivers holding non-domiciled CDLs who haven't been vetted by the Postal Inspection Service. The DOW has not implemented an equivalent safeguard. The USPS is ahead of the Department of War on driver vetting for its freight network.

NASA: Aerospace Freight

NASA aerospace freight carriers, 94 in total, show a 24.8 percent all-inspection OOS rate. For an agency shipping precision instruments, satellite components, rocket motors, and classified aerospace hardware, one in four trucks failing inspection should be considered an unacceptable risk to mission-critical cargo.

Space and Aerospace Freight: The SPACEFORCE-2 Intelligence Findings

Tea Technologies extended its federal freight analysis to the space and aerospace domain, identifying 1,029 space-tagged inspections across 594 distinct carriers hauling for launch providers (SpaceX, ULA, Blue Origin), aerospace defense primes (Lockheed Martin, Northrop Grumman, Raytheon, L3Harris), NASA centers, Space Force installations, and missile defense agencies.

Space/Aerospace Category Summary

Subcategory	Inspections	Carriers	OOS	Violations	Hazmat
Launch Provider	515	204	94	507	3
Aerospace Defense	316	254	82	477	3
NASA	52	48	17	73	0
Space Force	10	7	5	9	0
Launch Range	6	5	0	3	1
Missile Defense	3	3	1	6	0

Launch providers dominate volume with 515 inspections across 204 carriers, representing the SpaceX, ULA, and Blue Origin supply chains that move rocket components, propellants, satellite payloads, and launch infrastructure across American highways. EZE Trucking LLC (DOT 475073) is the single largest launch-provider hauler at 168 inspections with a 0.6 percent OOS rate, operationally clean. At the other end, Starr Trucking LLC (DOT 3240755) and MOB Carriers Inc (DOT 2078484) sit at 50 percent OOS on aerospace and launch freight, immediate review candidates. Redding Lumber Transport Inc (DOT 134171) runs a 26.3 percent OOS rate across 19 aerospace-tagged inspections, a concerning rate for a sustained-volume carrier.

Space Force direct-shipper inspections are extremely small: 10 inspections across 7 carriers. Most USSF freight moves through DLA or aerospace defense prime intermediaries and is not labeled as Space Force on inspection records. This creates a visibility gap identical to the one documented in Army freight: the shipper name on the inspection record reflects the intermediary, not the ultimate defense customer. A foreign-domiciled carrier, Electro Opticas Superior SA de CV (DOT 559848), appears in the aerospace freight data with a 40 percent OOS rate across 5 inspections. A Mexican corporation hauling aerospace defense freight with two in five trucks failing inspection represents the same cross-border security gap documented in the Tododren analysis for military freight.

Space/Aerospace Carrier Crash Exposure

The 594 carriers in the space and aerospace portfolio were collectively involved in 132,600 crashes over 24 months, including 3,697 fatal crashes resulting in 4,327 fatalities and 57,948 injuries. Four hundred eight of the 594 carriers had at least one crash. The same crash attribution caveat applies: these crashes are fleet-wide, not specific to space/aerospace loads. But these are the carriers moving rocket motors, satellite components, classified payloads, and launch infrastructure for the U.S. space enterprise.

Space/Aerospace Violation Profile (Fleet-Wide)

BASIC Category	Violations	OOS	Carriers
Vehicle Maintenance	26,745	8,144	489
Unsafe Driving	7,473	1	346
Hours-of-Service	5,367	658	393
Driver Fitness	1,180	822	224
Hazardous Materials	386	109	47
Controlled Substances/Alcohol	80	76	39

Controlled substance and alcohol violations across the space/aerospace carrier fleet total 80 events with 76 OOS, a 95 percent OOS conversion rate. Thirty-nine carriers in the pool that hauls launch vehicles, satellite payloads, and classified aerospace hardware have had drivers cited for drugs or alcohol in the cab.

Crash Exposure Across Federal Portfolios

The crash exposure for the federal freight carrier portfolio is extraordinary. Carriers confirmed to have participated in government/DOD freight movement were involved in 211,888 crashes over a 24-month period, including 5,381 fatal crashes resulting in 6,102 fatalities. The DHS portfolio alone accounts for 21,014 crashes, 539 fatal, with 563 fatalities.

These numbers require context. They do not mean that 6,102 people died in crashes while the carriers were hauling government freight. The FMCSA crash system does not identify shipper attribution at crash time. What these numbers mean is that the carriers the government is entrusting with its freight have, collectively, a crash portfolio that includes 6,102 deaths over two years. These are the companies that the DFTS contract, federal procurement, and the broader government freight system have selected, vetted, and continue to use. Their aggregate safety record is the government's revealed risk tolerance.

VIII. CARRIER PORTFOLIO ANALYSIS: DOD AND DHS FREIGHT HAULERS

DOD Portfolio: 38 Carriers Scored by Tea Technologies

Metric	Count	%
Total DOD carriers scored	38	100%
TEA Tier: Baseline	12	31.6%
TEA Tier: Monitor	21	55.3%
TEA Tier: Review	6	15.8%
Chameleon flags	3	7.9%
Hazmat authorized	7	18.4%
FMCSA Unrated	10	26.3%
Insurer: HIGH RISK	5	13.2%
HOS BASIC alert	9	23.7%
Driver Fitness alert	7	18.4%
Vehicle Maint. alert	5	13.2%
Crashes (24 months)	156	
Fatal crashes	11	
Fatalities	15	
Injury crashes	53	

Source: Tea Technologies DOD Carrier History, May 15, 2026

National Van Lines (DOT 76628), hauling for the Department of Defense, USAF, and National Guard, produced 10 OOS conditions across 8 government freight inspections (125 percent OOS rate), resulting in 24 violations. Its broader profile shows 400 percent vehicle OOS and 100 percent driver OOS rates with HOS, Driver Fitness, and Vehicle Maintenance BASIC alerts active. This carrier is hauling military freight with a safety profile that no responsible fleet manager would tolerate.

North American Van Lines (DOT 70851) recorded 29 crashes, including 2 fatal, in 24 months. It is insured by ACE American at the HIGH RISK tier. Twenty-nine crashes and two deaths in two years. This carrier hauls DOD freight.

Associated Petroleum Carriers (DOT 104701) hauls defense fuel at 66.7 percent vehicle OOS with 17 crashes, 2 fatal. Defense fuel. Two-thirds of its trucks fail vehicle inspection. Two fatal crashes. Minimum insurance.

DHS Portfolio: 18 Carriers Scored

Metric	Count	%
Total DHS carriers scored	18	100%
HOS alert	8	44.4%
Driver Fitness alert	6	33.3%
Vehicle Maint. alert	5	27.8%
Insurer: HIGH RISK	3	16.7%
Chameleon flags	1	5.6%
Crashes (24 months)	106	
Fatal crashes	3	
Fatalities	3	

Source: Tea Technologies DHS Carrier History, May 15, 2026

Twin Butte Trucking (DOT 2804935), operating with 9 power units, has all four BASIC alerts active (HOS, Driver Fitness, Vehicle Maintenance, and Unsafe Driving) while hauling DHS freight. All four. There is no BASIC category left to alert on. Every measurable dimension of safety is flagged. This carrier is hauling for the Department of Homeland Security.

Webley Express (DOT 3012380), based in Ontario, Canada, carries chameleon and authority transfer flags while moving DHS freight across the international border.

IX. GEOGRAPHIC RISK MAPPING AND MOVEMENT PATTERN ANALYSIS

State	Inspections	OOS	OOS Rate	Violations
Wyoming	302	134	31.1%	570
Missouri	744	332	27.6%	1,643
Tennessee	748	290	27.1%	684
Maryland	719	294	24.5%	1,019

State	Inspections	OOS	OOS Rate	Violations
Kentucky	885	310	23.4%	1,127
Iowa	605	164	22.8%	1,198
Washington	975	290	21.9%	1,604
Arizona	701	214	21.1%	1,608
California	2,566	644	18.1%	3,106
Texas	1,059	248	17.4%	1,653
Ohio	1,082	227	15.6%	1,284
New Mexico	1,991	283	12.0%	1,117

Source: Tea Technologies, top states by volume and OOS rate

London, Kentucky, remains the most extreme geographic hotspot: 299 government freight inspections, 183 OOS, 453 violations, and a 61.2 percent OOS rate. More than six in ten trucks hauling government freight through this corridor are placed out of service. London sits at the intersection of I-75 and the Daniel Boone Parkway, a corridor connecting the southeastern military installation complex to the Midwest logistics network. The consistent failure rates at this location indicate either a population of fundamentally deficient carriers serving this corridor or an enforcement environment that, when it does inspect, finds catastrophic conditions that exist everywhere but are only documented here.

Carrier Movement Patterns: Origin to Failure

Carrier Home State	Inspection State	Inspections	OOS	OOS Rate
Texas	Tennessee	20	19	95.0%
Washington	Washington	22	14	63.6%
Illinois	Washington	22	14	63.6%
Alabama	Alabama	25	11	44.0%
California	Arizona	40	17	42.5%
Texas	Texas	113	47	41.6%
Illinois	Montana	24	8	33.3%
Texas	Colorado	19	6	31.6%
California	California	88	20	22.7%

Source: Tea Technologies, carrier domicile vs. inspection state on military freight

Texas-domiciled carriers inspected in Tennessee had a 95 percent OOS rate. Twenty inspections, 19 out of service. Nineteen out of twenty trucks. This corridor-specific failure rate indicates that a particular population of Texas-based carriers serving the Tennessee military freight network is effectively non-functional from a safety standpoint.

X. INSPECTION LEVEL ANALYSIS: WHAT HAPPENS WHEN THEY ACTUALLY LOOK

Level	Description	Inspections	OOS	OOS Rate	Violations
1	Full 37-step (vehicle + driver)	6,618	3,284	49.6%	16,484
2	Walk-around (vehicle + driver)	10,945	3,743	34.2%	19,566
3	Driver-only (credentials/logs)	12,783	725	5.7%	10,863
4	Special study	20	8	40.0%	38
5	Terminal (vehicle only)	8	5	62.5%	26

Source: Tea Technologies, government freight inspections by level

This table is the single most important analytical finding in this assessment. When a CVSA-certified inspector conducts a full Level I, 37-step North American Standard Inspection on a government freight vehicle, including brake measurements, tire condition, frame and suspension checks, coupling devices, lighting, and a complete driver credential and log review, 49.6 percent of those vehicles are placed out of service. Half fail.

The aggregate OOS rate looks lower only because Level III inspections (driver-only, no vehicle examination) comprise the largest volume and produce only a 5.7 percent OOS rate. The Level III rate is low because the inspector never opens the hood or crawls under the truck. The vehicles are not being examined. They are being waved through with a credential check.

The implication for DOW freight is direct. A fleet manager who discovered that half his trucks failed a full inspection would ground the fleet. The DOD does not have a fleet manager for its contracted surface freight. It has a $2.3 billion contract with Crowley and hundreds of different carriers cycling through military installations.

XI. QUARTERLY TREND ANALYSIS: GOVERNMENT FREIGHT SAFETY IS DETERIORATING

Period	Inspections	OOS	OOS Rate	Driver OOS	Vehicle OOS	Violations
2023 Q1	1,204	332	27.6%	71	261	1,992

Period	Inspections	OOS	OOS Rate	Driver OOS	Vehicle OOS	Violations
2023 Q2	2,349	567	24.1%	115	452	3,857
2023 Q3	2,326	583	25.1%	117	466	3,531
2023 Q4	2,469	575	23.3%	123	452	3,670
2024 Q1	2,689	683	25.4%	129	554	4,406
2024 Q2	2,180	519	23.8%	83	436	3,224
2024 Q3	2,531	620	24.5%	104	516	3,931
2024 Q4	2,677	654	24.4%	129	525	4,048
2025 Q1	2,752	738	26.8%	151	587	4,409
2025 Q2	2,787	785	28.2%	183	602	4,680
2025 Q3	2,707	741	27.4%	167	574	4,023
2025 Q4	2,843	758	26.7%	176	582	4,013
2026 Q1	857	210	24.5%	61	149	1,184

Source: Tea Technologies, quarterly government freight OOS analysis

The trend is unambiguous. Government freight OOS rates averaged approximately 23-25 percent through 2023 and early 2024. Beginning in Q1 2025, rates escalated to 26.8 percent, peaked at 28.2 percent in Q2 2025, and remained elevated through Q4 2025 at 26.7 percent. The 2025 average OOS rate across all four quarters was 27.3 percent, compared with 2024 and 2023 averages of 24.5 percent. Government freight safety deteriorated by 11 percent between 2024 and 2025.

Driver OOS conditions have increased in parallel, from 83 in Q2 2024 to 183 in Q2 2025, a 120 percent increase. Vehicle OOS rose from 436 to 602 over the same period, a 38 percent increase. The deterioration is across both categories but is accelerating faster on the driver side, suggesting that the CDL fraud, medical examiner fraud, and ELD manipulation pipelines documented later in this report are beginning to manifest in the roadside inspection data.

XII. THE SUBCONTRACTING CHAIN: 251 CARRIERS FOR ONE SHIPPER

Shipper	Unique Carriers	Inspections	Ratio
US ARMY	251	306	1.22
US MILITARY	173	199	1.15
MILITARY	82	97	1.18

Shipper	Unique Carriers	Inspections	Ratio
US NAVY	73	81	1.11
US AIR FORCE	58	70	1.21
DOD	126	218	1.73
DEPARTMENT OF DEFENSE	39	62	1.59
OSHKOSH DEFENSE	34	44	1.29
US ARMY RESERVE CMD	27	29	1.07
DODSON VALCO	27	27	1.00
RED RIVER ARMY DEPOT	19	21	1.11
NATIONAL GUARD	13	13	1.00

Source: Tea Technologies, unique carriers per military shipper name

When the National Guard shows 13 different carriers across 13 inspections, that is 13 loads, 13 different companies, zero repeat engagement. When the US Army Reserve Command shows 27 carriers across 29 inspections, that is essentially a new carrier every time. The security clearance at the prime contractor level means nothing if a different, unknown carrier shows up at the depot for every load.

The Crowley DFTS contract expanded its carrier network by 500 percent. This data shows where that expansion leads: hundreds of carriers cycling through military loads with no continuity, no relationship, no safety baseline, and no accountability.

XIII. CARGO INTEGRITY AND GOVERNMENT PROPERTY RISK

Cargo Integrity Violation Surface

Category	Events	OOS	OOS Rate	Carriers	Avg Sev	Max Sev
Cargo securement, general	1,238	1,085	87.6%	706	2.75	3
Tie-down devices	1,646	820	49.8%	608	3.41	5
Shifting / falling cargo	737	509	69.1%	442	6.40	9
Hazmat placard/securement	1,116	473	42.4%	226	5.67	12
Intermodal container	218	212	97.2%	76	4.27	9
Railroad crossing	51	0	0%	46	4.92	5
Cargo tank spec/inspection	23	0	0%	19	7.00	7

Source: Tea Technologies, cargo integrity categories across federal freight portfolio (7,451 carriers)
The combined cargo-integrity surface across the government freight carrier portfolio comprises 5,029 events, 3,099 OOS orders, and approximately 1,800 unique carriers. The 61.6 percent aggregate OOS conversion rate means that when an inspector identifies a cargo integrity issue on a government freight vehicle, the condition is severe enough to require immediate remediation nearly two-thirds of the time. General cargo securement violations convert at 87.6 percent OOS. Nearly nine in ten. These are trucks where cargo is improperly secured, unsecured, or inadequately restrained. On government freight, the cargo is government property: military equipment, ammunition, defense materiel, agency supplies, scientific instruments. An 87.6 percent OOS conversion rate means that the securement failures inspectors are finding are not borderline. They are catastrophic.

Intermodal container securement violations convert at 97.2 percent OOS. Of 218 intermodal container securement events, 212 resulted in immediate out-of-service orders. Intermodal containers on flatbed or chassis equipment are the primary mode for moving military cargo through the port complexes that serve as force projection platforms. The SDDC 841st Transportation Battalion coordinates this freight through Charleston. Their carriers produced a 100 percent OOS rate. The intermodal securement data shows why.

Shifting and falling cargo events, coded under 393.100B and 393.100C, carry a maximum severity weight of 9 and convert at 69.1 percent OOS. Government property is literally at risk of falling off the vehicles carrying it.

Highest-Severity Violations in the Cargo Integrity Surface

Code	Description	Events	Max Severity
172504AHMPS	Bulk hazmat package not placarded	33	12
177834AHMC	HM not blocked/braced/secured as required	118	12
177823AHMPMCNP50	50%+ of required hazmat placards missing	86	12
393100BC	Cargo not secured against leaking/spilling/blowing/falling	424	9
393100CC	Cargo not secured against shifting	224	9
393126BCIM	Improper securement of intermodal containers	99	9
393134BCRHLC	Improper roll-on/hook-lift container securement	37	9
177817E2HMHC	Hazmat shipping papers not readily accessible	73	9

Source: Tea Technologies, fmcsa_violations, highest severity codes in cargo integrity surface
Severity 12 violations are the most severe in the FMCSA violation hierarchy. They are reserved for hazmat placarding and securement conditions that create immediate risk of release, exposure, or catastrophic incident. The federal freight carrier portfolio contains 237 severity-12 violations. These are not paperwork issues. These are conditions where hazardous materials, including potentially military explosives, propellants, and chemical agents, are being transported without required placards or without being properly blocked, braced, or secured.

XIV. HAZMAT ON DEFENSE LOADS: AMMUNITION, FUEL, AND EXPLOSIVES

Among pure DOD and military freight, hazmat inspections involve some of the most sensitive cargo in the military supply chain. Mecca Trucking LLC (DOT 3173438) was inspected while hauling Federal Ammunition in Saint Paul, Minnesota, and was found to have 12 violations. Bestway Transport (DOT 1800651) was hauling Winchester Ammunition inspected in Georgia. HOT Trucking LLC (DOT 1200566) was hauling from McAlester Army Ammunition Plant in New Mexico with 4 violations. Preferred Distribution Services (DOT 1885915) was hauling for U.S. Army P4525 with 15 violations, including 4 driver violations and 11 vehicle violations.

The Defense Logistics Agency appeared as the shipper on 19 hazmat inspections. Holston Army Ammunition Plant, which manufactures RDX and HMX military explosives, appeared on 12. Red River Army Depot on 3 with 2 hazmat OOS. The SDDC 841st Transportation Battalion in South Carolina had 4 hazmat violations.

Multiple Mexican-domiciled carriers (SA de CV entities) appear in the hazmat data hauling Titan Marine Fuel, with hazmat violation counts of 4-5 per inspection. Foreign-domiciled carriers hauling hazmat loads on routes that may intersect with military fuel supply chains represent a security gap that no existing screening mechanism addresses.

The DTR Part II, Chapter 205 explicitly restricts brokers, DFTS sub-TSPs, and freight forwarders from handling Class 1 Divisions 1.1 through 1.6 munitions and arms. The inspection data contains hazmat violations on carriers hauling ammunition and explosives from military ammunition plants. Either the DTR restrictions are being circumvented, or the carriers hauling these loads are operating under direct contracts that should provide more robust oversight than the data reflects.

XV. POST-ACCIDENT DOD FREIGHT: CRASHES ON MILITARY LOADS

Date	DOT	Carrier	Shipper	State	OOS	Viols	GVW (lbs)
2026-01-15	4161311	WrightXpress Special Svcs	US Military	PA	1	2	121,000
2025-10-30	2381163	Stallion Transportation	LVI Army	TN	0	0	122,000
2025-09-19	2496390	Noble Transport	Utah Army Natl Guard	IA	0	7	121,220
2025-08-20	4124812	BKM Enterprises	US Army Reserve CMD	TN	1	1	25,350

Date	DOT	Carrier	Shipper	State	OOS	Viols	GVW (lbs)
2025-06-16	3501919	Bjornsen Trucking	Oshkosh Defense LLC	IN	0	0	132,000
2025-05-01	2803020	Holland Rig Leveling	US DOD/Navy	AZ	0	9	135,250
2025-04-15	3173438	Mecca Trucking	Federal Ammunition	MN	0	12	120,000
2025-03-19	1800651	Bestway Transport	Winchester Ammunition	GA	0	1	120,000
2025-02-14	204961	Greentree Transportation	U.S. Navy	OH	0	3	133,500
2024-11-05	4128369	RAR Trucking	DOD	CA	0	2	118,000
2024-03-14	3229663	Wernham Livestock	Oshkosh Defense	MT	3	29	132,000

Source: Tea Technologies, POST_ACC_IND = Y, DOD/military shippers

Wernham Livestock LLC (DOT 3229663) crashed in Montana while hauling for Oshkosh Defense at 132,000 pounds gross vehicle weight. The post-accident inspection produced 29 violations and 3 out-of-service conditions, including 3 driver OOS. A livestock carrier hauling military tactical vehicles, crashing, and producing 29 violations at the crash scene. The name alone tells a story about subcontracting opacity: a livestock company hauling Oshkosh JLTVs.

Mecca Trucking crashed in Minnesota hauling Federal Ammunition at 120,000 pounds and produced 12 violations. An ammunition carrier crashing and producing 12 violations. Holland Rig Leveling crashed in Arizona hauling for DOD/Navy at 135,250 pounds and produced 9 violations.

The gross vehicle weights in this table are telling. Most loads are at or above 120,000 pounds. These are heavy-haul military freight movements involving vehicles at or exceeding legal weight limits, operated by carriers that are crashing and producing catastrophic violation counts at the crash scene.

XVI. VIOLATION TYPE ANALYSIS: WHAT DOW FREIGHT CARRIERS ARE ACTUALLY BEING CITED FOR

Major Violation Categories Across the Federal Freight Portfolio

Category	Violations	OOS Events	OOS Rate
Vehicle maintenance	166,003	48,894	29.5%

Category	Violations	OOS Events	OOS Rate
Tire violations	–	19,975 (OOS)	~76%
Hours of service	34,239	–	–
False log / ELD / RODS	23,648	–	–
Driver fitness	8,322	5,759	69.2%
Controlled substances/alcohol	543	530	97.6%
Invalid CDL / No CDL	2,543	~2,289	~90%
Speeding (severity 10)	4,176	–	–
Hand-held phone	951	–	–
English language proficiency	2,562	–	–

Source: Tea Technologies, fmcsa_violations across federal freight carrier portfolio (7,451 carriers)

Vehicle maintenance violations dominate the federal freight carrier portfolio with 166,003 total events and 48,894 OOS determinations. This is not a paperwork problem. These are mechanical deficiencies on trucks that have been documented as hauling government freight.

Tire violations alone produced 19,975 OOS events at approximately 76 percent OOS conversion. A tire at less than 50 percent of rated inflation is an imminent blowout. At highway speeds on an 80,000-pound vehicle hauling military cargo, a blowout can be catastrophic.

The 23,648 false log, ELD, and records-of-duty-status violations indicate that nearly 24,000 times, carriers in the government freight ecosystem were caught with falsified or manipulated driving time records. Falsified logs mean fatigued drivers. Fatigued drivers on military loads with logbooks showing compliance is a threat that ELD self-certification was supposed to eliminate. It has not.

The 2,543 invalid CDL or no-CDL events, with approximately 90 percent OOS conversion, mean that over 2,500 times, drivers operating in the government freight carrier pool were caught without the foundational legal credential for operating a commercial motor vehicle.

The 2,562 English language proficiency enforcement events are operationally significant. A driver who cannot read a bill of lading, communicate with base security, respond to emergency instructions, or understand hazmat shipping papers is an operational liability on any load. On military freight, particularly loads requiring TPS or involving classified material, language barriers create security vulnerabilities that transcend simple compliance.

Controlled substance and alcohol violations converted at 97.6 percent OOS across 543 events. When drugs or alcohol are found in the cab of a government freight carrier, the driver is removed from the road 97.6 percent of the time. The 2.4 percent that did not result in OOS are unexplained.

XVII. CONTROLLED SUBSTANCES AND ALCOHOL: DRUGS IN THE CAB ON DOW FREIGHT

Date	DOT	Carrier	Violation	Description
2026-02-28	125550	Atlas Van Lines	392.4A-DOSP	Drugs: operate CMV while in possession
2025-10-22	77949	United Van Lines	392.4A-DOSP	Drugs: operate CMV while in possession
2025-10-22	125550	Atlas Van Lines	392.4A-DOSP	Drugs: operate CMV while in possession
2025-07-27	77949	United Van Lines	392.5A3-IDUI	Alcohol in possession while on duty
2025-01-23	77949	United Van Lines	392.4A-DOSP	Drugs: operate CMV while in possession
2024-08-28	77949	United Van Lines	392.4A-POS	Narcotics/amphetamine possession on duty

Source: Tea Technologies, Controlled Substances/Alcohol BASIC, DOD carriers

United Van Lines (DOT 77949), a Missouri-based carrier with 4,731 power units and a Tea Technologies risk score of 49.4, had drivers cited for controlled substance or alcohol violations four times in eighteen months: narcotics and amphetamine possession in August 2024, drug possession in January 2025, intoxicating beverage possession on duty in July 2025, and drug possession again in October 2025. This is not an isolated incident. This is a pattern. Four substance violations in a year and a half. This carrier hauls for the Department of Defense. It holds a Satisfactory safety rating from FMCSA. Nobody pulled its DOW freight privileges after the first violation, or the second, or the third.

Atlas Van Lines (DOT 125550), which hauls for Total Military Management, the entity that coordinates military household goods shipments for service members and their families, had drivers cited for drug possession in October 2025 and again in February 2026. Total Military Management moves the personal belongings of military families during PCS relocations. The drivers moving those families' belongings had drugs in the cab.

XVIII. SIGNAL CONVERGENCE: WHEN ISOLATED FINDINGS BECOME OPERATIONAL INTELLIGENCE

The concept of signal convergence is central to this assessment. When a carrier or network repeatedly surfaces across crashes, cargo theft, insurance churn, identity changes, severe violations, unsafe driving, OOS patterns, authority instability, securement failures, and subcontracting opacity, that convergence itself becomes operational intelligence. Isolated findings treated in isolation are compliance data. The same findings mapped to the same carriers, addresses, insurers, and ownership structures become a threat picture.

Consider the convergence pattern that emerges from the DOD carrier portfolio:
National Van Lines (DOT 76628) converges across 125 percent government freight OOS, 400 percent vehicle OOS, 100 percent driver OOS, HOS alert, Driver Fitness alert, Vehicle Maintenance alert, and

military shipper exposure (DOD, USAF, National Guard). Any single one of these indicators might be dismissed. Together, they constitute a carrier that should not be hauling military freight under any circumstances.
Twin Butte Trucking (DOT 2804935) converges across all four BASIC alerts, 9 power units, and DHS freight exposure. A 9-truck company with every safety category flagged is hauling for the Department of Homeland Security.

The carriers hauling for the SDDC 841st Transportation Battalion converge across 100 percent OOS, 76 violations, 10 different carriers, 11 inspections, and the Charleston Strategic Seaport, one of DOD's designated force projection platforms. Ten different carriers, all failing, all at the same strategic chokepoint.

Signal convergence is not a statistical coincidence. It is the natural output of a system that does not cross-reference its own data. The FMCSA safety system, the DOD procurement system, the DFTS carrier network, the insurance system, and the authority registration system each contain fragments of the same picture. Nobody assembles the fragments. Tea Technologies does. The findings in this assessment are the result of that assembly.

The principle applies beyond individual carriers to network-level patterns. When carriers sharing addresses, phone numbers, insurers, or ownership structures also share crash patterns, OOS patterns, and violation patterns, the network itself becomes an intelligence target. The chameleon carrier investigations documented in this assessment (Super Ego, Compass Holding, Singh Organization, Armenian ghost fleet) all exhibit network-level signal convergence. The same analytical framework should be applied to the DOW freight carrier ecosystem.

XIX. THE CDL CRISIS: FRAUD, MILLS, AND THE MANUFACTURED WORKFORCE

The commercial driver's license is the foundational credential for operating an 80,000-pound vehicle on American highways. It is the only barrier between an unqualified individual and the cab of a truck hauling military freight. That barrier is compromised at every level.

The Scale of CDL Fraud

FMCSA has closed 550 training schools after 1,500 site visits and removed 3,000 third-party testing providers from the Training Provider Registry, with an additional 4,500 on notice. These are not marginal operations on the fringe of the industry. These are organizations that were registered with the federal government, authorized to train and test commercial drivers, and found to be producing fraudulent results at scale.

The Washington Skyline CDL School in Woodbridge, Virginia operated a cash bribery pipeline. Gold envelopes containing $520 to $530 were passed to examiner Jason Hodson for each passing score. Of 877 drivers Hodson tested, 80 percent failed the retest when given a legitimate examination. One hundred ten licenses were revoked. At least one fatal crash has been linked to Hodson's pipeline. The school reopened in Oregon.

In Bay County, Florida (June 2025), two DMV employees sold commercial driver's licenses to undocumented immigrants through a CubaMax franchise. $120,000 was seized. The operation sold the licenses to individuals who could not legally drive in the United States.

In Massachusetts, Sergeant Gary Cederquist of the Registry of Motor Vehicles fixed CDL tests for applicants he described in text messages as "brain dead" in exchange for personal favors including a driveway installation and Twizzlers. His code word for a fixed test: "golden handshake."
Rob Carpenter's CDL Fraud Factory investigation for FreightWaves documented 6,000+ fraudulent licenses linked to 13 deaths. Convicted CDL fraud operators averaged less than 2 years of actual enforcement consequences before disappearing from the system. The fraud pipeline does not produce individual failures. It produces classes of unqualified drivers who enter the commercial driving pool with credentials that the system treats as legitimate. When those drivers haul DOW freight, the security clearance at the prime contractor level is meaningless because the driver behind the wheel obtained his license through a criminal enterprise.

The Entry-Level Driver Training Collapse

The ELDT mandate, which took effect February 7, 2022, was supposed to standardize commercial driver training. It requires completion of a training program at an FMCSA-registered provider before a driver can take the CDL skills test. The Training Provider Registry was designed to ensure quality. It has instead become a vector for fraud. Of the 550 schools closed, many had been operating for months or years, producing graduates who are now driving commercially with fraudulent training certificates. FMCSA's removal of 3,000 third-party testing providers represents an acknowledgment that the testing system was compromised at industrial scale.

The third-party examiner pipeline is particularly concerning. FMCSA allows states to authorize non-government examiners to conduct CDL skills tests. These examiners operate with minimal oversight, setting their own schedules, choosing their own testing routes, and passing or failing applicants with limited verification. The Washington Skyline case is not an anomaly. It is the documented version of a pattern that exists wherever third-party testing operates without continuous oversight.

XX. THE NON-DOMICILED CDL CRISIS AND NATIONAL SECURITY

On December 9, 2025, Yisong Huang, a 54-year-old Chinese national, rear-ended a tractor-trailer on I-40 in Tennessee while watching a video on his phone. The chain-reaction crash killed Kerry Smith, a 31-year-old American trucker. When the Tennessee Highway Patrol administered an English proficiency test, Huang failed it. Huang entered the United States illegally through Mexico in 2023. He admitted to Border Patrol agents that he was a Chinese citizen who had crossed unlawfully. The administration released him and issued work authorization papers and a Social Security card. Eight months before he killed Kerry Smith, New York issued him a Class B commercial driver's license.

In November 2025, ICE arrested Akhror Bozorov in Kansas. Bozorov is an Uzbek national wanted since 2022 for membership in a terrorist organization. He obtained a Pennsylvania non-domiciled CDL in July 2025. It was a Real ID. The federal SAVE system cleared him. A wanted jihadist recruiter obtained a

commercial driver's license, a Real ID, through the same system that credentials the drivers hauling DOW freight.

Transportation Secretary Sean Duffy's subsequent audit found that more than half of New York's non-domiciled CDLs were issued illegally. He threatened to withhold $73 million in federal highway funds unless New York revokes them. California faces similar pressure. Since June 2025, more than 9,500 drivers have been placed out of service for failing English proficiency requirements under 49 CFR 391.11(b)(2) that were on the books but unenforced for nearly a decade.

Six states issue CDLs regardless of immigration status. The non-domiciled CDL pathway creates a direct conduit from illegal border crossing to the cab of a commercial vehicle. The FMCSA registration system does not screen CDL applicants against the Section 1260H Chinese Military Companies list. It does not cross-reference CDL applications with intelligence community watch lists beyond the SAVE system, which cleared a wanted terrorist. The USPS has announced it will phase out contracted drivers holding non-domiciled CDLs who haven't been vetted by the Postal Inspection Service. The DOW has not implemented an equivalent safeguard.

XXI. ENGLISH LANGUAGE PROFICIENCY: THE REQUIREMENT NOBODY ENFORCED

FMCSA Section 391.11(b)(2) is explicit. Drivers must be able to read and speak English sufficiently to converse with the general public, understand highway traffic signs and signals, respond to official inquiries, and make entries on reports and records. This requirement existed for decades. It was not systematically enforced until June 2025.

The 2,562 English language proficiency enforcement events documented in the federal freight carrier portfolio represent a belated acknowledgment that the requirement had been functionally suspended. The enforcement surge since June 2025 has resulted in 9,500+ drivers placed out of service. These are drivers who were operating commercial vehicles, including vehicles hauling government and military freight, without the ability to read a bill of lading, communicate with base security, understand emergency instructions, or respond to official inquiries at military installations.

Personnel at receiving facilities on military installations have reported watching drivers hand over bills of lading they could not read, using translation apps to communicate with base security. These are not isolated incidents. The non-domiciled CDL pipeline, combined with the industry's chronic driver shortage and carriers' willingness to hire anyone with a CDL regardless of language capability, has produced a population of drivers who do not meet the minimum regulatory standard for operating a commercial vehicle, let alone hauling freight to and from military installations.

The DTR Part II, Chapter 205 requires TOs to communicate with drivers, verify shipment documentation, and ensure compliance with security protocols. When the driver cannot read the documents or communicate with the TO, the security protocol is theater.

XXII. MEDICAL EXAMINER FRAUD AND THE NATIONAL REGISTRY

The DOT medical certificate is the second foundational credential for commercial driving. A driver must be physically qualified under 49 CFR Part 391, Subpart E, to operate a commercial motor vehicle. Physical qualification is determined by a medical examiner listed on the FMCSA National Registry of Certified Medical Examiners. The National Registry was compromised from inception.

Documented fraud mills and their operators include: Ranee Roberts (Missouri), who directed unqualified staff to perform examinations she was supposed to conduct. Joann Wingate (Pennsylvania), who issued medical certificates after her license was suspended. Biersmith, who forged a chiropractor's name on 65 certificates without holding a license. Dr. Surya at JFK Medport, whose assistants signed his name on certificates while he dealt oxycodone. Demetri Dearth, who fabricated every drug test result from his desk without ever collecting a sample.

The DOT OIG documented 33 indictments and 27 convictions related to medical examiner fraud by 2020. A single fraud mill takedown invalidated 6,000 medical certificates. Six thousand drivers who had been operating commercial vehicles with fraudulent physical qualifications were identified from one enforcement action. The scope of undetected fraud is unknown.

The NRCME Integration Initiative, first published in 2015, pushed three times, finally went live in June 2025 and immediately entered the waiver cycle. Eight states, including California and New York, are noncompliant with the integration requirements. The 2025 CVSA Roadcheck identified 493 OOS violations for medical certificate issues.

A legitimate DOT physical examination takes 30 to 45 minutes. Examiners processing hundreds of certifications monthly are not conducting examinations. They are selling paper. The drivers they certify enter the commercial driving pool with medical conditions that should disqualify them: uncontrolled diabetes, untreated sleep apnea, cardiovascular conditions, vision deficiencies, and substance abuse disorders that a proper examination would identify. When those drivers haul DOW freight, the medical certificate they carry is a fiction. The physical qualification it represents does not exist.

XXIII. SUBSTANCE ABUSE PROFESSIONAL AND CLEARINGHOUSE FRAUD

The FMCSA Drug and Alcohol Clearinghouse launched in January 2020 to create a centralized database of commercial driver substance abuse violations. When a driver tests positive or refuses a test, the result is reported to the Clearinghouse. The driver cannot return to safety-sensitive functions until a Substance Abuse Professional evaluates them and they complete a return-to-duty process.

SAP fraud has reopened the revolving door the Clearinghouse was designed to close. Documented operators include Wayne Hudson, Brandon Blackburn, and Zeph Nealy. The most instructive active case involves Ronelle Brockington and CoviLab in Charlotte, North Carolina. Brockington's professional credentials are Phlebotomist and Project Management, neither of which qualifies under 49 CFR 40.281

to serve as a Substance Abuse Professional. CoviLab's website advertises handling Clearinghouse uploads to "clear your record." An individual known as "Tap" is making Clearinghouse entries. The operation is under active investigation.

The Clearinghouse records what gets reported. It cannot verify whether the evaluation actually occurred, whether the SAP is qualified, or whether the return-to-duty testing was legitimate. A fraudulently cleared driver re-enters the commercial driving pool, and the Clearinghouse shows a clean record. That driver may bid on DOW freight loads through the DFTS carrier network. Nobody checks whether the SAP evaluation was real.

XXIV. ELECTRONIC LOGGING DEVICE MANIPULATION AND CAN BUS CYBERSECURITY

The ELD Self-Certification Problem

The ELD mandate requires electronic logging devices on all commercial motor vehicles. There are 1,133 registered ELD devices. The registration process is self-certification. No government testing. No independent verification. No cybersecurity requirements. The manufacturer states that its device complies with the technical specifications. FMCSA lists it. That is the entire process.

Twenty-seven ELD registrations were revoked in 2026, 38 in 2025. Revoked manufacturers have re-registered under new names within days. The same device, produced by the same people, with the same firmware, appears on the registry under a new brand name. The ELD registry has a chameleon carrier problem of its own.

The EMI fleet (Orland Park, Illinois), a 207-truck Serbian-American operation, maintained a Telegram group for coordinating log resets. Facebook advertisements offer ELD manipulation services for $30 per week. 58,382 false records of duty status violations were cited in 2025. CVSA designated ELD tampering as the 2026 International Roadcheck focus. New OOS criteria effective April 1, 2026 impose a 10-hour OOS penalty for tampered devices. FMCSA enforcement on ELD violations is up 28 percent. Fines of up to $16,000 per willful violation.

For DOW freight, falsified ELDs mean fatigued drivers on military loads with logbooks showing compliance. The ELD is supposed to prevent exactly this scenario. It does not, because the devices themselves are neither tested nor trustworthy.

CAN Bus Cybersecurity

The Controller Area Network bus is the internal communication system in every modern commercial vehicle. It connects the engine control module, transmission, brakes, steering, and all electronic systems. The CAN bus protocol was designed in 1983. It has no authentication mechanism. Any device connected to the CAN bus can send commands to any other device on the network.

The ELD mandate placed internet-connected devices on every truck's CAN bus. 1,133 devices, many manufactured overseas, many with wireless connectivity, all with access to the vehicle's core operating systems, and none subject to cybersecurity testing or certification.

Academic research has demonstrated remote takeover of steering, braking, and acceleration through CAN bus exploitation. A compromised truck is not merely a data vulnerability. It is a remotely guided weapon. For DOW freight, the question is straightforward: can an adversary compromise a vehicle carrying military cargo through the ELD supply chain? Nobody has tested this question against the 1,133 registered devices. The self-certification model ensures that nobody will, unless the government changes the model.

XXV. CHAMELEON CARRIERS AND IDENTITY CYCLING

Super Ego Holding

CBS 60 Minutes, April 12, 2026: FMCSA Administrator Derek Barrs called Super Ego Holding "the most notorious chameleon scheme" the agency has confronted. The Serbia-connected operation cycled through DOT authorities, creating new carrier identities after enforcement actions. Twin Carrier LLC (DOT 3518735), one of the entities in the network, compiled 62 crashes, 2 fatal, and 646 out-of-service orders while operating in CH Robinson's carrier pool. Drivers were altering DOT numbers on truck doors to match whatever authority was currently active.

Administrator Barrs reported at MATS 2026 that FMCSA had identified 400 to 500 carriers registered at addresses with no physical presence. Signal Hill, California: approximately 700 companies registered at one 2,000-square-foot building with a "No Trucks Allowed" sign on the parking lot. Dallas: 20+ carriers at a PhysicalAddress.com virtual mailbox.

Compass Holding

Compass Holding (Clarendon Hills, Illinois) represents the most sophisticated infrastructure model documented. The network includes Compass Funding, Compass Payment, Compass Equipment Finance, Compass Truck Rental, and Compass Specialty Insurance RRG. UCC liens filed by Compass entities are maintained 18 months post-OOS enforcement. New financial instruments appear on successor entities within 13 days of enforcement action against predecessor entities. The network creates, finances, insures, and recycles carriers within its own closed ecosystem, making external detection extremely difficult.

Singh Organization

The Singh Organization (San Bernardino, California) used fraudulent operating authorities to intercept and steal electronics shipments. Federal charges included conspiracy, wire fraud, identity theft, and money laundering. The organization demonstrated that the same authority system exploited by chameleon carriers for safety evasion can be exploited for cargo theft.

Armenian Ghost Fleet

Serj Gevorgyan allegedly built a multi-million dollar freight fraud operation using ghost carriers, stolen identities, and fabricated operating authorities. The investigation documented systematic identity theft of legitimate carriers' USDOT credentials to book and steal loads. Two $30 million government shipments of computer chips were stolen by Armenian theft networks and never recovered.

Three chameleon flags exist in the scored DOD carrier portfolio. The same authority system these organizations exploit is the system through which DOW freight carriers obtain operating rights. When a chameleon carrier shuts down one authority and opens another, the new authority is immediately eligible to receive DOW freight tenders through the DFTS network. No automated cross-referencing prevents this. No manual review catches it in real time.

XXVI. POLITICAL ACCESS AND REGULATORY CAPTURE

Dragos Sprinceana, operator of GoldCoast Logistics and the DMG carrier network, compiled 150+ crashes, 10 fatalities, and $889,630 in defaulted fines while maintaining an aggressive political donation profile. Federal Election Commission records show $134,992 in donations from 2020 to 2024. RNC: $35,500. Matt Gaetz: $9,500 (contributed 4 days after a fundraiser). Mike Waltz: more than $20,000 (same-day contributions while in default on federal fines). Sprinceana attended election night at Mar-a-Lago in November 2024. He met incoming National Security Advisor Waltz on January 13, 2025. He attended a 700-person gala in April 2025. No FARA registration on file.

When a carrier network responsible for 10 fatalities and nearly $900,000 in unpaid federal fines has direct personal access to senior national security officials, the term "regulatory capture" is inadequate. This is operational access. The same individual whose fleet has killed 10 people on American highways is in the room with the people who set the national security agenda.

The political access dynamic is not limited to Sprinceana. It reflects a broader pattern in which the trucking industry's political engagement infrastructure, its PACs, its association lobbying, and its individual donor relationships, operates independently from its safety and compliance performance. A carrier's political donation history is not visible to the FMCSA analyst reviewing its safety data. A carrier's crash record is not visible to the political official accepting its donation. The systems are disconnected by design, and that disconnection creates the space in which a fleet with 10 fatalities can operate at the intersection of political access and regulatory impunity.

XXVII. CHINESE PENETRATION OF U.S. TRANSPORTATION INFRASTRUCTURE

In January 2008, the American Trucking Associations hosted a delegation from the China Road Transport Association. The visitors, representing the Highway Transportation Administration Bureau, Beijing XiangLong Assets Management, and Guangxi Wuzhou Communications, spent two days meeting with ATA leadership and major carriers including Con-way Freight, Roadway, and RoadLink. They studied U.S. trucking operations, truck safety regulations, driver training, federal and state tax structures, and environmental regulations.

Seventeen years later, the Pentagon added COSCO Shipping to the Section 1260H Chinese Military Companies list. COSCO, the fourth-largest ocean carrier in the world, operates joint venture container terminals at the ports of Los Angeles, Long Beach, and Seattle. The company moved nearly 40 million TEUs to and from U.S. ports. A MITRE analysis published in February 2024 found that Chinese companies own or operate terminals in 100 ports across 60 countries.

Shanghai Zhenhua Heavy Industries Company (ZPMC) manufactures 70 percent of container cranes globally. Those cranes constitute 80 percent of the cranes in U.S. ports, including 10 Strategic Seaports designated by the Department of Defense for military deployments.

LOGINK, China's National Transportation and Logistics Public Information Platform, provides the Chinese government with visibility into shipping and supply chains and the ability to track shipments of U.S. military cargo on commercial freight.

Parallel to the port penetration, Chinese companies have purchased agricultural land near military installations. The Fufeng Group purchased 370 acres near Grand Forks Air Force Base in North Dakota, a facility with intelligence, surveillance, and reconnaissance capabilities. Chinese companies own nearly 10,000 acres in Polk County, Florida, near MacDill Air Force Base. Another 277 acres sit in San Diego County near Camp Pendleton. A Chinese energy company subsidiary purchased land near Laughlin Air Force Base, the Air Force's largest pilot training facility.

The 2024 NDAA Section 805 will prohibit DOD from directly procuring from 1260H entities, effective June 2026. Section 851 of the 2025 NDAA prohibits DOD from contracting with companies that employ lobbyists for 1260H entities. The indirect prohibition extends to June 2027. There is no systematic screening of DOW freight carriers against the 1260H list. The non-domiciled CDL pathway that produced the Huang and Bozorov cases is available to any foreign national. CRRC, a Chinese state-owned rail manufacturer now on the 1260H list, secured $4.3 billion in U.S. transit rail contracts. General Adams warned Congress that Chinese rail penetration would provide early warning of U.S. military mobilization. The dots connect. Chinese-operated port terminals. Chinese-manufactured cranes at Strategic Seaports. Chinese logistics platforms tracking military cargo. Chinese farmland near air bases with ISR capabilities. Chinese nationals obtaining CDLs through non-domiciled pathways. A carrier network that expanded 500 percent for DOW freight with no 1260H screening. The vulnerability is not theoretical. It is structural, and it has been in place for over a decade.

XXVIII. CYBER-ENABLED STRATEGIC CARGO THEFT

On April 30, 2026, the Federal Bureau of Investigation published Public Service Announcement I-043026-PSA warning that cyber-enabled strategic cargo theft was surging. In 2025, estimated cargo theft losses in the United States and Canada reached nearly $725 million, a 60 percent increase from 2024. Confirmed incidents increased by 18 percent. The average value per theft rose 36 percent to $273,990, driven by more selective, high-value targeting.

The FBI documented the multi-step scheme: threat actors compromise broker and carrier email accounts through spoofed URLs and phishing emails. The phishing websites download remote monitoring and management (RMM) software, giving threat actors total, undetected access to brokers' and carriers' systems. Using compromised accounts, they post fraudulent listings on load boards in the

tens of thousands. Legitimate carriers bid on fake loads and are themselves compromised through malicious carrier broker agreements. Posing as compromised carriers, the threat actors accept real shipments, double-broker the loads to partially unwitting drivers, provide manipulated bills of lading, change delivery destinations, and steal the cargo for resale.

The threat actors change the legitimate carrier's contact information with FMCSA and update insurance information to permit loads the carrier previously did not accept. The compromised carrier may not realize the infiltration until brokers contact them about missing loads booked under their authority without their knowledge.

On February 5, 2026, the U.S. Attorney's Office for the District of Massachusetts charged Romoy Forbes, a 31-year-old Jamaican national living in Deer Park, New York, with a multi-state organized cargo theft conspiracy. Co-conspirators hacked into carrier email accounts and, posing as the legitimate carriers, contracted with shippers for loads. Forbes arrived at warehouses pretending to work for the hacked carriers, loaded goods, and drove away. The stolen goods included 33,750 pounds of frozen snow crab worth $325,000, pallets of blueberries, and $433,830 of designer cologne. Forbes sold stolen goods to his phone contact labeled "My customer for everything."

The same techniques that enabled Forbes to steal snow crab can intercept military freight. The load board system, the FMCSA registration system, and the carrier identity verification system are the same for commercial freight and government freight. A threat actor who compromises a carrier's FMCSA profile and books a military load through the DFTS network can redirect that load to an alternative destination. The FBI's warning is not hypothetical. Two $30 million government shipments of computer chips were stolen by theft networks and never recovered.

XXIX. FMCSA PROFILE HACKING AND DIGITAL IDENTITY THEFT

The FMCSA carrier profile is the digital identity of every registered motor carrier, broker, and freight forwarder. It contains the USDOT number, contact information, insurance certificates, safety ratings, and operating authority. Load boards, brokers, and shippers rely on this data to verify carrier legitimacy. Hackers increasingly target FMCSA accounts using stolen USDOT PINs, phishing emails, and brute-force attacks. Once inside, they change contact information to impersonate the legitimate carrier, upload forged W-9s and insurance certificates, pose as the carrier on load boards to book freight, and hire real truckers to haul loads before disappearing with the cargo.

A hacked FMCSA profile creates cascading consequences: cargo theft under the legitimate carrier's name, insurance claim denials because the profile was used fraudulently, DOT compliance issues from unauthorized profile changes, and loss of broker and shipper trust even when the carrier is the victim. When an impersonator fraudulently signs the Bill of Lading, the legitimate carrier may not be legally liable for the stolen cargo, but they face litigation because cargo insurance policies hinge on the legal liability established by a valid BOL.

In reported cases, scammers impersonated three different carriers in a single day, stealing from multiple shippers. Law enforcement struggles to keep pace, leaving brokers and carriers to self-police the problem. FMCSA profile security is a compliance issue because a compromised profile can lead to

regulatory violations, insurance disputes, and operational shutdowns. Transportation companies must treat their digital credentials with the same care as physical assets.

For DOW freight, the FMCSA profile hacking threat means that a carrier approved for military loads could be impersonated. The impersonator books the military load. A real driver, partially unwitting, picks up the freight. The cargo is redirected. The chain of custody is broken. The DTR's advance shipment planning and verification requirements exist precisely to prevent this scenario, but they depend on the FMCSA profile data being trustworthy. When the profile itself is compromised, the verification process verifies a fiction.

XXX. INSURANCE, FINANCIAL RESPONSIBILITY, AND THE RRG CRISIS

The federal minimum insurance requirement for motor carriers is $750,000, unchanged since 1980. Adjusted for inflation, that 1980 dollar amount is approximately $2.2 million in 2026 dollars. The insurance floor has not been updated in 46 years. The median truck crash jury verdict is now $36 million. Wabash 2024: $462 million. Florida 2021: $1 billion. ATRI documents 3.7 percent annual growth in tort filings. The Garcia-Tran bill proposes raising the minimum to $5 million. An FMCSA Notice of Proposed Rulemaking is expected to propose $2 million or higher.

Five Risk Retention Groups are currently flagged at COLLAPSE RISK by Tea Technologies insurer intelligence. RRGs are the last-resort insurance mechanism for carriers that cannot obtain conventional coverage. They are organized under the Liability Risk Retention Act of 1986, which preempts state insurance regulation and allows RRGs to operate across state lines with limited oversight. When an RRG collapses, every carrier it insures loses coverage simultaneously, and every active claim against those carriers becomes potentially unrecoverable.

Universal Casualty, identified in the Tea Technologies insurer scoring as a HIGH RISK insurer, is writing coverage for carriers with 30+ crashes. Five DOD carriers and three DHS carriers are insured by HIGH RISK-rated insurers. The insurance backing DOW freight is, in multiple documented cases, provided by insurers whose financial condition and underwriting practices would not survive scrutiny from a commercial risk manager.

The insurance ecosystem interacts with the chameleon carrier problem. Compass Specialty Insurance RRG, part of the Compass Holding network documented in this assessment, provides insurance within the same closed ecosystem that creates, finances, and recycles carriers. When the insurer and the carrier are controlled by the same network, the insurance is not a risk transfer mechanism. It is a compliance artifact that satisfies the FMCSA registration requirement without providing meaningful financial protection.

The Supreme Court's 9-0 ruling in Montgomery v. Caribe Transport (May 14, 2026) created state tort liability for freight brokers in carrier selection. Brokers dispatching carriers with catastrophic safety records now face direct litigation exposure. The DFTS contract operates through the same brokerage system. Crowley tenders loads to carriers and subcontractors whose safety records are documented in this assessment. The Montgomery ruling means that the entire freight brokerage chain, from Crowley

through its carrier network to the subcontractors and owner-operators who actually move the freight, is now exposed to state tort liability for negligent carrier selection.

XXXI. INTERMODAL SECURITY: RAIL, MARITIME, AND CRITICAL INFRASTRUCTURE

The Defense Transportation System depends on civilian rail, ports, and airports for force projection. SDDC designates 40,000 miles of rail as the Strategic Rail Corridor Network (STRACNET) connecting 140+ military bases to seaports. The military operates 1,350 railcars on privately owned track.

The Foundation for Defense of Democracies documented Volt Typhoon's persistent access to U.S. transportation systems. Volt Typhoon, a Chinese state-sponsored cyber threat group, has maintained access to critical infrastructure including transportation networks, positioning for potential disruption during a military contingency.

The Alliance for American Manufacturing and Guardian Six Consulting's "Remaking American Security" report (2013) documented the defense supply chain's vulnerability to foreign dependency at every level: raw materials, subcomponents, and end items. The report's central finding, that DOD lacks visibility below the prime contractor level, applies directly to surface freight. DOD knows it contracted with Crowley. It does not know who Crowley hired. The supply chain visibility gap that General Adams warned about for semiconductors, specialty metals, and lithium-ion batteries exists in identical form for the physical movement of those same materials.

TSA's Trucking Security and Incident Response Training (T-START) program has not been funded since FY2009. There are 521,000 active interstate freight carriers with zero formalized security training. No carrier in the DFTS network is required to undergo transportation security training. The TSA Surface Division maintains oversight authority for surface transportation security but lacks the resources and legislative mandate to extend meaningful security requirements to the freight trucking sector.

XXXII. VEHICLE RAMMING AND SURFACE TERRORISM

The Mineta Transportation Institute database documents 8,440 attacks on surface transportation worldwide since 1970. Within the United States, 83 vehicle ramming attacks have occurred since 2012. Between November 2024 and May 2025, 27 attacks killed 76 people. New Orleans, January 1, 2025: 14 killed in the deadliest U.S. ramming attack.

The connection to trucking is direct. Timothy McVeigh rented a Ryder truck, used a fake ID, and killed 168 people in Oklahoma City. Sayfullo Saipov, who killed 8 on the West Side Highway in New York, held a CDL and FMCSA operating authority. Akhror Bozorov, arrested in November 2025 for terrorist organization membership, was driving commercially with a Pennsylvania non-domiciled CDL when ICE found him. He was not driving a passenger vehicle. He was operating a commercial motor vehicle. Eleven million registered trucks operate on American roads. TSA trucking security has been unfunded since 2009. The Vehicular Terrorism Prevention Act was introduced in February 2025 but has not been enacted. The DFTS carrier network does not screen for terrorism-related indicators beyond whatever

baseline appears in the standard FMCSA registration process. A wanted terrorist recruiter cleared that process and obtained a Real ID and a CDL. The system that is supposed to prevent this failed at the most basic level.

XXXIII. THE HISTORY THAT EXPLAINS THE PRESENT: FROM STAGECOACHES TO CHAMELEONS

The American freight system is not a modern invention. It is an ancient one that has been retrofitted, expanded, deregulated, digitized, and ultimately hollowed out over the course of three centuries. Understanding what the industry is today requires understanding what it was at the beginning, not because the history is quaint, but because the same human impulses that produced the first freight crimes in colonial America are producing the same crimes right now.

The argument of Rob Carpenter's investigative book "The Hitchhiker's Guide to Trucking" is direct: the stagecoach robber and the chameleon carrier are the same person, separated by 150 years of technology and nothing else. The road agent who robbed a Wells Fargo stage in 1875 relied on the inability of law enforcement to verify identity across jurisdictions. Cross into the next territory and you became whoever you said you were. The chameleon carrier who shuts down a USDOT number in 2024, registers a new authority the following week under a marginally different name, and restarts the same operation from the same address with the same trucks relies on the same structural vulnerability.
The regulated era (1935-1980) solved the identity problem almost by accident. When getting operating authority required years of effort, public testimony, and survival of protests from competitors, the barrier itself filtered out bad actors. Not because regulators were good at spotting criminals, but because the process required sustained engagement, local presence, and a paper trail that made anonymity nearly impossible. A carrier's certificate of public convenience and necessity was worth hundreds of thousands of dollars because it represented years of work and a documented operating history. By 1978, approximately 17,000 motor carriers operated under ICC regulation, and the freight community was contained enough that a bad actor's record would catch up with him eventually.
On July 1, 1980, President Jimmy Carter signed the Motor Carrier Act and removed most of the restrictions that had governed the industry for 45 years. By most measures of efficiency, the Act delivered. Freight rates fell. Service options expanded. Intermodal shipping flourished. What nobody fully grasped was what else had been removed along with the regulatory barriers. Within a decade of deregulation, the number of motor carriers more than doubled. Today, more than 800,000 motor carriers hold active operating authority. That is a 47-fold increase from the regulated era. The agency responsible for overseeing them has roughly 1,000 employees.

The 2012 GAO study found that 1,136 new applicants in a single year exhibited chameleon characteristics: shared addresses, phone numbers, and ownership patterns with previously sanctioned carriers. Eighteen percent of suspected chameleons had been involved in severe crashes, compared to six percent of non-chameleon carriers. Three times the crash rate. Same highways. Different names.
A fraudster with an internet connection, a burner phone, and $2,000 for a bond premium can access billions of dollars in freight. The FMCSA registration system does not require biometric authentication. Operating authority can be obtained with minimal documentation verification. Safety records are stored separately from registration and insurance records. A carrier can be put out of service, and the same

owner can register a new company with a new authority, operating the same trucks from the same address, without triggering automatic alerts.

Private enterprise fills the enforcement gap because public enforcement is inadequate. Wells Fargo hired the Pinkertons for the same reason. When the official accountability system fails, the market creates a workaround. The workaround costs money, which legitimate operators pay and fraudulent ones ignore. This is the basic economic structure of freight fraud, and it has been the same since the first road agent stopped the first stage.

XXXIV. THE CONTESTED LOGISTICS FRAMEWORK: THREAT, ENVIRONMENT, SELF

ARTRANS is not facing a narrow compliance or automation problem. It is confronting a contested logistics challenge shaped by adaptive threats, a complex commercial environment, and internal structures optimized for a world that no longer exists.

The Irregular Warfare Center's three-lens framework, Threat/Environment/Self, provides the organizing construct for understanding why existing approaches have been insufficient and what must change. The threat is not static. State and non-state actors adapt faster than compliance cycles can respond. A carrier that is vetted at contract award may be compromised, sold, or identity-cycled before the next periodic review. Static vetting mechanisms designed for a permissive environment cannot keep pace with adversaries operating continuously.

The environment is fragmented. No single organization possesses complete visibility or authority. FMCSA regulates carriers but does not control who hauls DOD freight. DOD contracts for freight but cannot enforce FMCSA regulations. Installation TOs are on the front line but lack real-time visibility into carrier safety status, insurance validity, or identity history. The data that would enable integrated risk assessment exists across multiple systems that do not communicate.

The self-assessment is the hardest lens. The institutional posture is optimized for efficiency and throughput. Procedural compliance is conflated with operational assurance. The assumption that a valid operating authority, a current insurance filing, and a Satisfactory safety rating constitute adequate vetting for DOW freight has been disproven by every data table in this assessment. The governance architecture evolved more slowly than the threat environment.

The planned continuing effort through the NDTA Fall Meeting (October 2026, Grapevine, TX) and the Transportation Advisory Board engagement (Spring 2027), with a charter, objectives, lines of effort, and recommendations developed through monthly coordination sessions, represents the institutional mechanism for bridging these gaps. The May 19, 2026 breakout session is the initial convening event. The strategic timeline extends through 2027. The threats documented in this assessment will not wait for the timeline to complete.

XXXV. LOADVERIFI: CRYPTOGRAPHIC CHAIN-OF-CUSTODY FOR FREIGHT SECURITY

The vulnerabilities documented throughout this assessment converge on a single structural problem: the absence of verified, continuous, tamper-proof chain of custody from freight origin to destination. The DFTS contract tracks loads through Crowley's TMS. The TMS records dispatch, tracking, and proof-of-delivery. What it does not verify is the physical identity of the driver, the physical condition of the vehicle, or the physical integrity of the cargo at every point of transfer. The system trusts whoever is named on the paperwork. It does not verify who actually moves the freight.

LoadVerifi (loadverifi.com), developed by Tea Technologies, is a cryptographic chain-of-custody verification system designed to close this gap. The system operates on a SHA-256 hash ledger that creates an immutable, cryptographic record from origin to destination.

How LoadVerifi Works

LoadVerifi operates through six verification stages, each producing a cryptographic hash that links to the next, creating an unbreakable chain of custody from booking to delivery.

- **Step 1: Create the Load.** The broker or shipper creates a LoadLedger with shipment details. The chain begins. Every load receives a unique cryptographic identifier at creation.
- **Step 2: Screen the Carrier.** LoadVerifi pulls real-time carrier intelligence from THE TEA Highway Intelligence platform: crash prediction scores, chameleon carrier detection, insurance status and insurer risk tier, BASIC scores, and nuclear verdict risk assessment. Red flags surface before the rate confirmation goes out.
- **Step 3: Verify the Driver.** The driver completes biometric identity verification through government ID scan and facial recognition. The system confirms CDL status, medical certificate validity, Clearinghouse status, and English proficiency in real time. Verified once, confirmed at every pickup.
- **Step 4: Secure the Pickup.** The driver arrives at the dock, opens a text link on their phone, scans the BOL, records the seal number, and confirms identity. Sixty seconds. Everything hashed into the chain.
- **Step 5: Track the Chain.** Every event from booking to delivery is timestamped and cryptographically linked. Equipment verified. Insurance confirmed. Seal numbers matched. Nothing can be altered after the fact.
- **Step 6: Prove Everything.** Export a litigation-ready audit trail showing every party, every document, every verification, and every hash. Mathematically provable. Court-admissible.

Who LoadVerifi Serves

- **For Brokers and Shippers:** Screen carriers against 2.2 million carrier intelligence records. Crash prediction, chameleon detection, and insurance verification at assignment. One workspace per load. Litigation-ready audit trail export with one click. Biometric proof of who picked up the load.
- **For Motor Carriers:** Demonstrate compliance and safety commitment. Differentiate from unvetted competitors. Reduce liability exposure through documented chain of custody.

- **For Drivers:** Simple, fast verification at pickup. No additional hardware. Text-link verification takes 60 seconds. Professional drivers who pass biometric verification gain competitive advantage.

At the point of origin, LoadVerifi captures and verifies four elements: the physical driver (biometric identification through facial recognition and document verification), the driver's credentials (CDL, medical certificate, hazmat endorsement, TWIC, and real-time Clearinghouse status), the drivers location regardless what GPS or telematics system they use, and the vehicle (VIN verification, DOT number confirmation, insurance status, and authority verification against FMCSA records).
Each verification event generates a SHA-256 cryptographic hash that is recorded on the LoadVerifi ledger. Essentially blockchain but for every element of the load. The hash cannot be altered retroactively. Any modification to the underlying data would produce a different hash, making tampering immediately detectable. The ledger is not a blockchain in the decentralized, cryptocurrency sense. It is a cryptographic chain-of-custody record maintained by Tea Technologies that provides the same immutability guarantee without the energy overhead and latency of distributed consensus.

At each point of transfer, including intermediate stops, cross-dock facilities, and driver changes, LoadVerifi re-verifies the driver, vehicle, and cargo integrity. Each verification event adds a new hash to the chain. The receiving party at the destination, or the system itself can verify the complete chain: every driver who touched the load, every vehicle that carried it, every transfer point it passed through, and the cryptographic proof that none of this information was altered after the fact.

What LoadVerifi Solves

The system addresses the driver identity gap (is the person behind the wheel who they claim to be?), the credential verification gap (are the driver's qualifications current and legitimate?), the vehicle identity gap (is this the vehicle that was dispatched?), the subcontracting opacity gap (how many hands touched this load between origin and destination?),the location gap, and the chain-of-custody gap (can anyone prove that the load was not compromised, diverted, or substituted in transit?).

For DOW freight, LoadVerifi provides the verification infrastructure that the DTR Part II, Chapter 205 requires but that the current system cannot deliver. The TO at the installation can verify, through cryptographic proof, that the driver who arrived is the driver who was dispatched, that his credentials are current and legitimate, that the vehicle matches the dispatched equipment, and that the load has not been transferred to unauthorized carriers in transit. The cost is typically less than $50 per shipment depending on volume. The alternative is the system documented in this assessment: 251 different carriers hauling for the US Army with no verification of who actually moves the freight.

XXXVI. MONTGOMERY v. CARIBE TRANSPORT AND ITS IMPLICATIONS FOR DOW FREIGHT

On May 14, 2026, the Supreme Court ruled 9-0 in Montgomery v. Caribe Transport that the Federal Aviation Administration Authorization Act's preemption clause does not bar state-law negligence claims against freight brokers for their selection of motor carriers. Justice Barrett, writing for the Court, held that the "safety exception" in FAAAA preemption preserves negligent hiring, selection, and retention

claims against brokers. Justice Kavanaugh's concurrence stated that preemption cannot create a "black hole" where no entity is accountable for safety.

The ruling transforms the legal landscape for freight brokerage. Every freight broker in the United States now faces state tort liability for the carriers it selects and dispatches. The plaintiff's bar will target brokers who dispatch carriers with known safety deficiencies. The carrier data in this assessment, 125 percent OOS rates, chameleon flags, four BASIC alerts, drugs in the cab, becomes admissible evidence in broker liability litigation.

The DFTS contract operates through the same brokerage system. Crowley tenders loads to carriers and subcontractors. Under Montgomery, Crowley and every broker in its network are now liable for the safety records of the carriers they select. Dispatching a carrier with a 125 percent OOS rate, or a carrier with four BASIC alerts, or a carrier whose drivers have been caught with narcotics four times in eighteen months, is now actionable negligence.

The DOW should leverage the Montgomery ruling by requiring DFTS brokers to implement carrier vetting standards that meet or exceed the thresholds being established by the plaintiff's bar. If the tort system can identify and sanction dangerous carrier selection, the DOW should at minimum match that standard for military freight. The data to do so exists. The platform to do so exists. The legal framework now demands it.

XXXVII. RECOMMENDATIONS FOR IMMEDIATE ACTION

These recommendations are operational requirements for securing DOW surface freight, designed for implementation within existing DOD acquisition frameworks.

1. Establish a DOW Approved Carrier Registry

Minimum Tea Technologies risk score thresholds. No chameleon flags. OOS rates below the national average. No Unsafe Driving or Controlled Substances BASIC alerts. Insurer rated MODERATE or better by Tea Technologies insurer intelligence. Apply to all subcontracting layers. Government Bills of Lading name the actual carrier, not just the prime contractor.

2. Attach Security Verification to the Load, Not Just the Contract

TWIC-equivalent vetting for every driver on DOW freight. Biometric verification at depot docks through IDEMIA, Persona, or equivalent platforms. Tea Technologies LoadVerifi for cryptographic chain-of-custody and end-to-end tracking. English proficiency verified at tender. The security clearance process that applies to the prime contractor must follow the freight through every subcontracting layer. When the load is classified, the chain of custody must be cryptographically verifiable from origin to destination.

3. Mandate Section 1260H Cross-Referencing

Automated, continuous screening of every carrier, subcontractor, and owner-operator against the Section 1260H Chinese Military Companies list. This screening should be automated within the DFTS

TMS and applied at the point of tender, not after the fact. Transportation Secretary as a permanent CFIUS voting member for any transaction involving freight and logistics companies with access to defense supply chains.

4. Third-Party ELD Testing and CAN Bus Security Standards

Replace the ELD self-certification model with mandatory third-party cybersecurity testing. Establish CAN bus security standards for DOW freight vehicles. Prohibit ELD devices manufactured by entities from 1260H-listed countries on DOW freight vehicles. The internet-connected device on the truck's CAN bus is the least-examined attack vector in the entire DOW freight security picture.

5. Postpayment Security Audits

Audit carrier identity, driver qualification, vehicle condition, and subcontracting compliance on DOW loads. Expand GSA Transportation Act audit authority from financial compliance to security compliance. Current audits verify that rates are correct. They do not verify that security requirements were maintained throughout the chain.

6. Integrate Carrier Intelligence Platforms

Tea Technologies, GenLogs, SearchCarriers, Highway, and Bluewire for real-time risk scoring, chameleon detection, insurer intelligence, and crash prediction. The Tea Technologies Federal Investigator Portal (.gov gated) was built specifically for federal law enforcement and logistics oversight. The platform provides real-time carrier scoring, insurer risk assessment, authority stability monitoring, and signal convergence alerts.

7. Fund TSA Trucking Security

T-START has been unfunded since FY2009. Security coordinator designation and observe-assess-respond training should be required for all DFTS network carriers at a minimum. 521,000 active interstate freight carriers operate with zero formalized security training. The TSA Surface Division maintains authority but lacks resources.

8. Reduce Subcontracting Layers

Cap subcontracting depth on DOW freight at one layer below Crowley. Require advance disclosure and approval of all subcontractors. Implement LoadVerifi chain-of-custody verification from tender to delivery. The current system allows unlimited subcontracting depth with no disclosure requirement.

9. English Proficiency Verification on DOW Freight

Require English proficiency verification for every driver hauling DOW freight, applied at the point of tender and verified at the point of loading. The USPS has implemented this for postal freight. The DOW should do the same for military freight.

10. Require Drug and Alcohol Clearinghouse Pre-Hire Query for DOW Freight

Require pre-employment Clearinghouse queries for every driver entering the DOW freight carrier pool, with verification that Substance Abuse Professional evaluations were conducted by qualified, verified SAPs. The current Clearinghouse does not verify SAP qualifications. The DOW should require that verification as a condition of carrier eligibility.

XXXVIII. CONCLUSION: THE SCALE OF WHAT IS BROKEN

The American commercial motor vehicle network is compromised at every level of regulatory oversight, driver credentialing, carrier vetting, vehicle integrity, and financial responsibility. The Department of War moves billions of dollars in freight through this compromised network every year. The data in this assessment documents the consequences.

Government freight carriers fail roadside inspections at rates far above the national average. Pure DOD freight is in worse condition than the broader government freight universe. The subcontracting chain has fragmented to the point where 251 different carriers show up under one shipper name. Carriers with 125 percent OOS rates, four BASIC alerts, drug-possession citations, and chameleon flags haul military freight. The SDDC unit coordinating force projection through a Strategic Seaport produced a 100 percent OOS rate. Foreign-domiciled carriers haul defense fuel and ammunition with OOS rates exceeding 100 percent. A wanted terrorist held a CDL and a Real ID. A Chinese national with an illegal border crossing and a New York CDL killed an American trucker. Two $30 million government shipments of computer chips were stolen and never recovered. The FBI reports that cyber-enabled cargo theft surged to $725 million. The ELD mandate placed unvetted, internet-connected devices on every truck's CAN bus with no cybersecurity testing. Chinese state interests operate port terminals, manufacture cranes at Strategic Seaports, and track military cargo through LOGINK. The federal minimum insurance has not been updated since 1980. Five RRGs are at collapse risk. Chameleon carriers cycle through identities faster than enforcement can act. Political donors with 10 fatalities and $900,000 in unpaid fines have direct access to national security officials.

This is not a theoretical risk. This is a documented operational reality. The scale of operational instability and systemic vulnerability inside American surface transportation is significantly worse than publicly understood.

The fix requires will. The data exists. The technology exists. The platforms exist. The legal framework, post-Montgomery, now demands it. The question is whether the institution will exist to match the scale of the problem. The threats documented in this assessment are not waiting for committees, charters, or timelines. They are operating today, on the highways, on the load boards, in the FMCSA registration system, and at the gates of military installations.

The stagecoach robber crossed into the next territory and started fresh. Today, he filled out a form online. The difference between 1875 and 2026 is not the crime. It is the scale.

Tea Technologies, Inc. robcarpenter@theteaintel.com | theteaintel.com | trucksafe.com
Tea Technologies, Inc. | May 2026

APPENDIX A: REFERENCES AND SOURCE MATERIALS

- Tea Technologies, Inc. Tea Technologies Highway Intelligence Platform. 8,183,916 inspections, 5,144,926 crashes. theteaintel.com. Patent-pending App. 64/009,415.
- Carpenter, Rob. “Dragon in the Cab: How China Quietly Embedded Itself in American Trucking.” FreightWaves, January 10, 2026.
- Carpenter, Rob. “Who’s Hauling Your DOD and Government Freight?” FreightWaves/X, January 23, 2026.
- Carpenter, Rob. “CVSA Roadcheck and Enforcement Are Crucial to National Security.” FreightWaves, May 12, 2026.
- Carpenter, Rob. The Hitchhiker’s Guide to Trucking: How We Built, Broke, and Can Still Save American Trucking. Amazon KDP, 2026.
- CBS 60 Minutes. Super Ego Holding investigation. April 12, 2026.
- CVSA. International Roadcheck Results 2019-2026. 2025: 56,178 inspections, 18.1% vehicle OOS.
- MITRE Corporation. Chinese Technology in U.S. Seaports. February 2024.
- Foundation for Defense of Democracies. Military Mobility Depends on Secure Critical Infrastructure. 2024-2025.
- Alliance for American Manufacturing / Guardian Six Consulting. Remaking American Security: Supply Chain Vulnerabilities and National Security Risks Across the U.S. Defense Industrial Base. May 2013.
- FBI. Public Service Announcement I-043026-PSA: Cyber-Enabled Strategic Cargo Theft Surging. April 30, 2026.
- U.S. Attorney’s Office, District of Massachusetts. USA v. Romoy Forbes: Multi-State Organized Cargo-Theft Conspiracy. February 5, 2026.
- Hylant. When Your FMCSA Profile Gets Hacked: The Hidden Cyber Threat to Transportation Companies. October 14, 2025.
- Mineta Transportation Institute. Global Terrorism Database: Surface Transportation Attacks.
- U.S. DOD. Section 1260H Chinese Military Companies List. January 2, 2025.
- U.S. Supreme Court. Montgomery v. Caribe Transport, Inc. May 14, 2026. 9-0.
- USTRANSCOM / Crowley Government Services. Defense Freight Transportation Services I and II. $2.3B, 7-year, 300K annual movements, 41 depots.
- Defense Transportation Regulation, Part II, Chapter 205: Transportation Protective Service. April 10, 2026.
- GAO. Chameleon Carrier Study, 2012. 1,136 new applicants with chameleon characteristics.
- DOT OIG. National Registry of Certified Medical Examiners Audit, 2019-2020.
- FMCSA. Training Provider Registry enforcement actions: 550 schools closed, 3,000 TPR providers removed, 4,500 on notice.
- FMCSA. ELD Registry: 1,133 devices, 65 revocations (2025-2026).
- FMCSA. Drug and Alcohol Clearinghouse.
- ATRI. Truck Tort Litigation Trends 2014-2023.
- NDTA-CAS. Surface Force Projection Meeting. Christopher Newport University, Newport News, VA. May 18-21, 2026.
- MG (Ret.) Edward Dorman. IWC/NDTA Coordination Meeting Minutes. May 13, 2026.
- MG (Ret.) Edward Dorman. ARTRANS and the Reality of Contested Logistics: Mini White Paper. February 2026.
- S10 Consulting / Irregular Warfare Center. Strategic Framing Themes and Proposed Timeline.
- NDAA 2024, Section 805 (1260H direct procurement prohibition).

- NDAA 2025, Section 851 (lobbyist prohibition for 1260H entities).

APPENDIX B: DEFENSE TRANSPORTATION REGULATION KEY PROVISIONS

DTR Part II, Chapter 205: Transportation Protective Service

Key restrictions relevant to this assessment:
Brokers, DFTS TSPs, sub-TSPs, freight forwarders, shipper agents, and shipper associations are restricted from handling Class 1 Divisions 1.1 through 1.6, sensitive munitions, arms, and shipments requiring Security Escort Vehicle Service (SEV), Protective Security Service (PSS), Rail Armed Guard Surveillance Service (ARG), Rail Inspection Service (RIS), Dual Driver Protective Service (DDP), Constant Surveillance Service (CIS), Trailer Tracking Service (DCS), Satellite Motor Surveillance Service (SNS), Greater Security Service (GSS), and Military Guard Personnel (MGP).
Canadian-based commercial drivers may transport goods to the United States from Canada if all goods were loaded in Canada and the Canadian companies have completed Level II (SECRET) facility and personnel security clearance requirements. Purely domestic service (point-to-point within the United States) is not permitted.
Transportation Officers are required to: conduct advance shipment planning; verify security clearances for personnel handling classified material; ensure DD Form 626 Motor Vehicle Inspection standards are met; coordinate with installation security and force protection officers; verify both signatures from team drivers on DD Form 1907; and ensure loads are transferred only to qualified drivers.
All personnel who accept, handle, package, or ship classified material must have a security clearance equal to or greater than the material being handled. Government personnel operating vehicles or providing security to AA&E, classified, and sensitive shipments must have a favorable NACLC adjudicated to interim or final SECRET clearance.

APPENDIX C: FEDERAL FREIGHT AGENCY PROFILES AND DATA STATUS

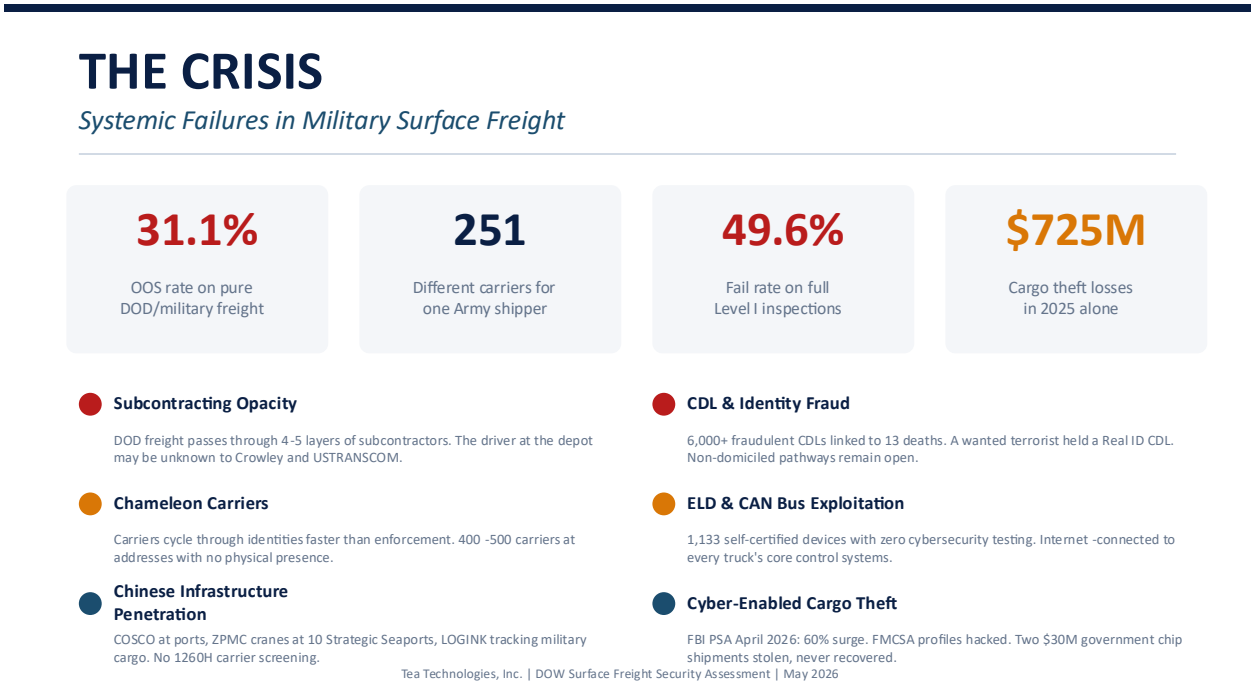
Confirmed Agency Profiles (Data Verified)

USDA / Forest Service: 414 inspections, 323 carriers, 31.9% OOS, 53.0% L1 OOS. Worst Level I OOS rate among confirmed federal civilian categories.
DOE / Nuclear Complex: 672 inspections, 379 carriers, 21.0% OOS, 38.8% L1 OOS. High-severity exposure for nuclear enterprise freight.
USPS: 740 inspections, 432 carriers, 19.2% OOS, 35.2% L1 OOS. Postal Service implementing non-domiciled CDL phase-out ahead of DOW.
DOI: 191 inspections, 152 carriers, 24.1% OOS, 39.4% L1 OOS. Interior Department freight, including national parks, BLM, and USGS.
GSA: 166 inspections, 106 carriers, 24.1% OOS, 23.1% L1 OOS. General Services Administration freight and supply chain.

NASA: 117 inspections, 94 carriers, 24.8% OOS. Aerospace and precision freight.
VA: 34 inspections, 26 carriers, 26.5% OOS. Veterans Affairs medical and supply freight.
State/Local: 2,617 inspections, 1,331 carriers, 17.4% OOS, 18.4% L1 OOS. Cleanest category among confirmed profiles.

Partial/Requiring Repopulation

DOD: 3,923 inspections, 2,611 carriers, 19.7% OOS, 29.2% L1 OOS. Partial due to acronym boundary refinement.
HHS: 736 inspections, 526 carriers, 20.1% OOS, 31.1% L1 OOS. Health and Human Services, CDC, NIH freight.
DOJ: 6,394 inspections, 3,752 carriers, 21.6% OOS, 30.3% L1 OOS. Partial due to acronym boundary issues.



THE IMPACT

What These Failures Mean for National Security and Mission Readiness

Force Projection Risk	Adversary Exploitation	Institutional Exposure
SDDC 841st Trans. Bn. at Charleston Strategic Seaport: 100% OOS rate	Foreign-domiciled carriers hauling defense fuel with 111% OOS rates	SCOTUS Montgomery ruling: brokers now liable for carrier selection (9-0)
Oshkosh Defense (JLTV manufacturer) carriers failing at 43-62% OOS	Chinese logistics platform LOGINK provides visibility into military cargo movements	Drivers with narcotics in the cab hauling DOD freight, 4 violations in 18 months at one carrier
Red River Army Depot: 47.6% OOS on the Army's only organic vehicle repair base	No systematic 1260H screening of DOW freight carriers or subcontractors	Five RRGs at collapse risk backing DOW freight carriers
211,888 crashes across government freight carriers in 24 months, 6,102 fatalities	Non-domiciled CDL pathway cleared a wanted terrorist with a Real ID	Government freight safety deteriorated 11% between 2024 and 2025

Tea Technologies, Inc. | DOW Surface Freight Security Assessment | May 2026

A SOLUTION

Operationalizing Freight Security Through Technology, Policy, and Verification

LoadVerifi: Cryptographic Chain of Custody

01 **Create the Load**
Unique cryptographic ID at booking

02 **Screen the Carrier**
Real-time TEA intelligence: crash prediction, chameleon detection, insurance

03 **Verify the Driver**
Biometric ID, CDL, medical cert, Clearinghouse, English proficiency

04 **Secure the Pickup**
BOL scan, seal number, identity confirmation. 60 seconds. Hashed.

05 **Track the Load and the Chain**
Every event timestamped and cryptographically linked origin to destination

06 **Prove Everything**
Litigation-ready audit trail. Mathematically provable. Court -admissible.

Immediate Recommendations

DOW Approved Carrier Registry
Minimum TEA score thresholds, no chameleon flags, insurer quality gates across all subcontracting layers

Section 1260H Cross-Referencing
Automated, continuous screening of every carrier and subcontractor against the Chinese Military Companies list

ELD Cybersecurity Testing
Replace self-certification with mandatory third -party testing. CAN bus security standards for DOW vehicles

Reduce Subcontracting Depth
Cap at one layer below Crowley. GBLs name the actual carrier. Advance disclosure required.

Fund TSA Trucking Security
T-START unfunded since FY2009. Security training for all 521,000 active interstate freight carriers

LoadVerifi cost: < $50 per shipment | loadverifi.com | theteaintel.com

Tea Technologies, Inc. | DOW Surface Freight Security Assessment | May 2026

END OF REPORT
Tea Technologies, Inc. | May 2026