



**SURFACE EXECUTIVE WORKING GROUP
MEETING MINUTES
25 July 2019**

NOTICE

One of the initiatives following the 2012 National Defense Transportation Association (NDTA) Forum was to establish a Surface Executive Working Group (EWG). The purpose of this EWG is to promote dialogue between government and industry while focusing on preserving readiness capability and ensuring the nation has access to necessary commercial transportation capability. Within the EWG, transportation issues of government and industry are studied and the statuses of the issues are reported at large. The EWG is led by co-chair: United States Transportation Command (USTRANSCOM), and the Military Surface Deployment and Distribution Command (SDDC). The body of the EWG consists of a cross-section of senior leader representatives from the surface industry, Department of Defense (DoD) and the Department of Transportation (DoT). Industry representatives of the EWG are determined by USTRANSCOM in collaboration with SDDC. Invites to all participants are based on agenda focus areas. NOTE: DoD officials participating in the EWG may not obligate the government contractually or make policy, nor may they transfer any authority or responsibility for government decisions to industry or to the industry members of the EWG. By making the minutes of EWG meetings available electronically, DoD, DoT, and NDTA promote the exchange of information to other forums. DoD invites interested parties to comment on issues considered at EWG meetings, to provide additional information, or to request further information.

ATTENDING INDUSTRY REPRESENTATIVES:

<u>Organization</u>	<u>Telephone</u>
Bennett International Group	(770) 862-1806
BNSF	(817) 867-0644
Boyle Transport	(978) 670-3408
CSX Transportation	(703) 861-3844
Crowley Maritime	(608) 519-6396
Landstar Transportation Logistics	(904) 390-4898
Mercer Transportation	(800) 626-5375
National Defense Transportation Association	(703) 751-5011



Norfolk Southern Corporation	(478) 258-0027
Northwest Seaport Alliance	(800) 657-9808
Port of Beaumont	(409) 835-5367
Port of Virginia	(757) 683-2105
Ports America	(912) 644-6123
Tri-State Motor Transit	(623) 344-1105
Union Pacific Railroad	(402) 544-4471
YRC Worldwide	(301) 797-5922

TASKS

The updated list of tasks from the EWG is at Attachment 1.

MEETING SUMMARY

Notes: (a) Where possible, this meeting summary is chronological synopsis of related discussions (See Attachment 2 for overall agenda). In some cases, individual questions/ comments are captured. In other cases, the paragraph summarizes a common thought/understanding. (b) The term "industry" appears in this document both in a collective sense (i.e., at large) as well as by mode (trucking, rail, and/or seaports). (c) In some cases, there are comments/points associated with individuals, while in others they are simply noted collectively e.g., "industry." The difference is for clarity, based on a single comment/point versus a more collective discussion. Comments/Points by individuals are not meant to imply there may be others in industry/industry mode who do/do not share the same view.

1. Opening Remarks. Vice Admiral Dee Mewbourne (TCDC)
 - a. Welcomed all attendees and briefed the group on the changes to structure and representation from previous Surface EWGs in order to facilitate a specific discussion set.
 - b. Desired meeting outcome is to better understand how industry and government can work together to support domestic surge operations in a complex contested environment to meet DoD requirements and priorities.



2. Review of Due Outs from Surface EWG July 2018

- a. Due outs were briefed by exception. Since the July 2018 meeting all 12 due outs from that meeting were “Closed” at the Surface EWG level and deposition/status documented (Attachment 1). Note: in some cases the action recommended was fully achieved and closed. In other cases, action(s) were assigned to be worked/resolved within the various offices/working groups as appropriate—back briefs (if required) would be by exception.
- b. Due out (#201401-3): Update Progress on Base Access for Trucking Providers, which originated in Jan 2014, remains open. COL Baird (OSD A&S) provided an update on the Services progress on implementing a more common internal and external physical security standard within the Services to improve base access for truck cargo/deliveries (Attachment 3 Base Access Update). Industry suggested a hotline when installation access delays cargo as a possible solution or to get guidance for cargo.

3. State of the Industry (Trucking). (Mr. Mike Cashner (Landstar))

- a. Briefed trucking expectations for 2019-2020:
 - i. Slower economic growth; Industrial Production > 1% in next 6 months
 - ii. Rates continue to fall –spot rates finish year 19% below 2018
 - iii. Utilization expected to bottom out around 93%
 - iv. Rates flat into 2020; there is a “floor”
 - v. Reduced hiring and new truck purchases
 - vi. Driver shortage stable into 1Q of 2020
- b. Things that might affect capacity (2019-2020):
 - i. Automatic on-board recording devices to Electronic Logging Device (ELD) mandate –DEC 2019
 - ii. Drug and Alcohol Clearing House –3Q of 2020
 - iii. Drug testing (hair follicle versus urinalysis) –mid 2020
 - iv. Reducing Commercial Driver’s License (CDL) age from 21 to 18 –TBD



- v. Rising insurance costs: “Nuclear verdicts”
- c. Summary
 - i. Large, diverse and fragmented industry
 - ii. SDDC’s core carriers have expansive networks which can help cover surges
 - iii. Rate increases in 2017 and 2018 allowed carriers to recover cost, increase compensation and update equipment
 - iv. Capacity will continue to loosen into 2020, but remain “tight” overall
 - v. Carriers view drivers as scarce resources and will provide competitive rates and preferred status to shippers who promote efficiencies
 - vi. Shippers & carriers can enhance efficiencies and assure capacity at competitive rates by collaborating on short and long term transportation strategies and capacity plans
 - vii. Pending regulatory action may further constrain capacity specifically in the areas of Electronic Logging Device and Drug Clearinghouse)
 - viii. We are all in this together
- 4. State of the Industry (Rail). (Ms. Theresa Lorinser (BNSF))
 - a. The rail sector anticipates they will also be affected by the uncertainty of the markets in much the same way as the trucking sector. This uncertainty may affect the rate of investment the rail industry makes to its infrastructure.
 - b. 850 new 100-ton 89’ chain flatcars with “Universal” chains were added in 2017 & 2018 and 400 were added to the fleet in 2019 to improve the military useful railcar fleet.
- 5. State of the Industry (Ports). (Mr. Ernest Bezdek (Port of Beaumont))
 - a. Discussed the importance of continued investment in seaport infrastructure and its impact the economy.
 - b. Port activity generates 30M jobs, and \$5.4T in economic value annually. This is up 7.6% and 4.3% annually since 2014 respectively.



- c. Discussed the need for industry to focus on increased labor recruitment and training in all aspects of the surface industry (truck, rail and port). Ports face continuing challenges due to very aggressive industrial development (especially in the gulf) and we compete for those workers. Industry partners should focus their efforts on recruitment of good, qualified new workers and then continuously train those new employees to promote a safe and efficient work force. The Port of Beaumont would be happy to work with industry partners on possible solutions.
6. Discussion Session #1: *Capacity Surge—Equipment, Facilities, and Manpower*. (Mr. Bruce Busler (TCAC/TEA))
- a. TCAC/TEA built upon previous surge deployment discussions to provide a better understanding of requirements and challenges in a plausible large-scale surge deployment scenario. The flow of deploying equipment from origins, to consolidation and training sites, and to seaports of embarkation was explained. The control and timing of flow within CONUS is critical to optimizing the sequenced delivery of units and their equipment into theater.
 - b. Surface Summary:
 - i. 59% Stons move by Rail (67,865 pieces/1.1M Stons/25M SqFt).
 - ii. 28% Stons move by Truck (64,094 pieces/502K Stons/19.8M SqFt).
 - iii. 13% Military Convoy Vehicles.
 - c. A large portion of surge deployment will be consumed by moving Guard and Reserve Forces to consolidation sites or training locations.
 - d. TEA described how it utilizes Programs for National Defense (Highways for National Defense; Railroads for National Defense; and Ports for National Defense) to address surge deployment challenges. This included a discussion on the DoD's reliance on both DOD-owned Defense Freight Railway Interchange Fleet (DFRIF) railcars and commercial railcars. A large scale contingency deployment would likely include over 30,000 loaded railcar moves and over 50,000 loaded truck moves.



- e. TEA described the Ports for National Defense Study and how Strategic Seaports are chosen, in order to ensure that sufficient and resilient seaport capacity is available on the west, east and gulf coasts.
 - f. Key points
 - i. Multiple “peak demand” periods requires careful management of railcars across CONUS.
 - ii. Time-definite truck use is important to meet timelines.
 - iii. High priority ammo flow coincident with deployment.
 - iv. Sustainment flow (containers) follows deployment 30 days later.
 - v. TEA is currently working with Federal Motor Carrier Safety Administration (FMCSA) on exemptions to Driver Hour Service and with the Federal Highway Administration (FHWA) / State DoTs on expediting oversize/overweight permitting during military emergencies.
 - vi. Industry stated TEA assumptions on the ability to pool removable gooseneck (RGN) trailers might need to be reviewed. (After the briefing TEA reviewed supporting simulation data and identified inaccuracies in the chart present, most notably the depiction of a peak demand for 600+ 4-axle RGNs). (Attachment 4 Updated RGN data slide)
7. Discussion Session #2: *Physical and Cyber Intrusions/Attacks; Technology Advances*. (Mr. Rob Brisson (TCJ3))
- a. Discussed how USTRANSCOM is plugged into the national cybersecurity infrastructure. Department of Justice (DoJ) is the lead department for threat response through Federal Bureau of Investigations (FBI) & National Cyber Investigative Joint Task Force (NCIJTF). Threat response activities include conducting appropriate law enforcement and national security investigative activity. Department of Homeland Security (DHS) is lead department for asset response through Certified Information Systems Auditor (CISA) & National Cybersecurity and Communications Integration Center (NCCIC). Asset response activities include:
 - i. Furnishing technical assistance to affected entities to protect their assets
 - ii. Mitigating vulnerabilities, and reduce impacts of cyber incidents



- iii. Identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities
 - iv. Assessing potential risks to the sector or region, including potential cascading effects
 - v. Developing courses of action to mitigate these risks and facilitating information sharing.
- b. Truck, rail, and ports (less stevedoring contractors) do not have the same contractual relationship as DoD has with the air and sealift carriers. USTRANSCOM and SDDC will research cyber “standard” for these modes. USTRANSCOM will share with industry (perhaps through NDTA). Current guidance would be for industry to follow/meet basic National Institute of Standards and Technology (NIST) 800-171 standards and become more self-aware of their cyber posture.
 - c. Mr. Morgan (DHS) informed the group all strategic ports are required [through their Area Maritime Security Committee (AMSC)] to conduct an annual cyber exercise. USTRANSCOM/SDDC should consider integrating within these cyber training opportunities. SDDC will follow-up with AMSC.
 - d. USTRANSCOM will follow up with updated USTRANSCOM Cybersecurity contact information and National Cyber Incident Reporting Plan. (Attachment 5).
8. Transportation Management System (TMS). (Mr. Andy Dawson (TCJ3))
- a. 24 month prototype window (March 2018 through February 2020).
 - b. Release 1.1 went live on 1 November; gained visibility of CONUS freight shipments.
 - c. Release 1.2 – four scenarios: two “Project the Force”; two “Sustain the Force.”
 - i. Fort McCoy – Assess TMS freight tendering Functionality.
 - ii. 3/25 Brigade Combat Team (BCT) – Joint Readiness Training Center (JRTC) Rotation – Assess TMS freight tendering functionality.



- iii. Determine functionality applicable to rail, Third Party Payment System (TPPS), HAZMAT, Ammo, Overweight/Over-Dimensional.
 - iv. Establish and evaluate carrier collaboration portal.
 - d. Release 1.3 – Defense Logistics Agency (DLA) / Air Channel Process.
 - i. Defense Freight Transportation Services (DFTS) lane – DLA San Joaquin to Travis AFB.
9. Closing Remarks.
- a. TCDC reviewed due outs (Attachment 1 Surface EWG Tasks) and thanked all for attending, affirmed there would be follow ups to the actions taken, and closed the meeting.

ATTACHMENTS:

1. Surface EWG Tasks
2. Surface EWG Agenda
3. Base Access Update
4. Updated RGN Trailer Data (Surge Brief)
5. Follow-up Cybersecurity Message

UPDATES/CORRECTIONS

Contact the USTRANSCOM J5-I point of contact at (618) 220-4948 or email: transcom.scott.tcj5j4.mbx.i-division@mail.mil for updates or corrections to these minutes.

COPIES OF ASSOCIATED BRIEFS

This meeting was discussion based with only a few conversation starter slides. Contact the USTRANSCOM J5-I point of contact at (618) 220-4948 or email: transcom.scott.tcj5j4.mbx.i-division@mail.mil for copies of the slides presented during this Surface EWG meeting.



ATTACHMENT 1 SURFACE EWG TASKS

New Tasks:

TASK	LEAD	DUE
(#201907-1) Assess the need for a carrier hotline when installation access delays cargo.	SDDC	Update 1 FEB 2020
(#201907-2) Confirm surge truck assumptions and requirements (specifically RNG trailer requirements and access to capacity) with industry.	SDDC/TEA	CLOSED via clarification of data with industry
(#201907-3) Evaluate ability to provide a routine meeting for the truck sector similar to other modes (e.g. sealift and rail) to coordinate future requirements.	SDDC	Update 1 FEB 2020
(#201907-4) Develop a strategy to train port laborers on how to operate specialized equipment.	SDDC / FORSCOM / Industry	Update 1 FEB 2020
(#201907-5) Evaluate the value of adding USCG to future Surface EWGs. Is there another suitable alternative?	USTRANSCOM / SDDC	Update 1 FEB 2020
(#201907-6) Evaluate the value of adding American Short Line Rail Road Association or Short Line representation to future EWGs.	USTRANSCOM / SDDC	Update 1 FEB 2020
(#201907-7) Collect pertinent cyber resource information and distribute to EWG members and NDTA.	USTRANSCOM	CLOSED (Attachment 5)
(#201907-8) Coordinate with Strategic seaport Area Maritime Security Committees (AMSCs) to integrate with their annual cyber exercises.	SDDC	Update 1 FEB 2020
(#201907-9) Research cyber "standard" for trucking, rail, and port industry (believe these modes lack contracts).	USTRANSCOM / SDDC	Update 1 FEB 2020



Ongoing Tasks:

TASK	LEAD	UPDATES DUE
(#201401-3) Update progress on base access for trucking providers. Request DASD(TP) to provide update as required.	OSD(A&S)	Next EWG

Tasks Closed Since Previous EWG:

TASK	LEAD	COMPLETED
(#201807-1) Identify metrics USTRANSCOM/ SDDC needs to track. How can or should they be tracked? [CLOSED]	Industry (NDTA Surface Committee)	There are industry resources and reports which provide capacity/availability / rates/trends which could be useful. Also, recommend DoD establish internal metrics to monitor the status of their core carriers: e.g. wait times at gates and in/around installations; arrival to load/offload; amount of tender offers accepted; amount of capacity commitment by awarded carrier vs what is actually provided.
(#201807-2) Provide BCT forecasts for steady state. [CLOSED]	USTRANSCOM / SDDC	Providing in multiple forums



U.S. TRANSPORTATION COMMAND

POINTS OF CONTACT
USTRANSCOM/J5-I (618) 220-4948
SDDC (618) 220-6507

<p>(#201807-3) Define how far in advance industry would need forecasting data to affect BCT movement (what is the desired outcome). [CLOSED]</p>	<p>Industry (NDTA Surface Committee)</p>	<p>Rail: current SDDC annual forecasts very helpful; 3-4 months for BCT. See also Surface EWG 2018 minutes Paras 5. b, c, d, and g.</p>
<p>(#201807-4) Identify efficiencies DoD could make to improve capacity? [Industry provided copy of slide used in previous NDTA Surface Transportation Committee Meeting.] [CLOSED]</p>	<p>Industry (NDTA Surface Committee)</p>	<p>Industry provided during Surface Transportation Committee Meetings 2018/2019; to also be covered in Surface EWG 2019 brief</p>
<p>(#201807-5) Reference (#201807-4), explore/further discuss suggested potential actions. [CLOSED]</p>	<p>USTRANSCOM / SDDC</p>	<p>Currently partnering with the OSD Chief Management Officer's Services & Category Management Reform Team and their contractor (Boston Consulting Group) on how the DoD can more effectively and efficiently operate in the domestic business lane.</p>
<p>(#201807-6) Engage with DoT (FHWA, FMCSA) to assess the feasibility of relaxing Hours of Service constraints to support surge deployment operations. [CLOSED]</p>	<p>SDDC TEA</p>	<p>TEA engaged with FMCSA, however progress has been slow and sporadic. Addressed in slides.</p>
<p>(#201807-7) Further discuss feasibility of relaxing Rail Hours of Service constraints to support surge deployment operations. [CLOSED]</p>	<p>SDDC TEA / Industry (NDTA Rail Sub-Committee)</p>	<p>Rail subcommittee to take on and dialog with FRA</p>



U.S. TRANSPORTATION COMMAND

POINTS OF CONTACT
 USTRANSCOM/J5-I (618) 220-4948
 SDDC (618) 220-6507

<p>(#201807-8) Coordinate with FHWA, State DOTs, and State Defense Movement Coordinators on implementing more efficient or even pre-coordinated/pre-approved oversize/overweight permitting. [CLOSED]</p>	<p>SDDC TEA</p>	<p>TEA has ideas on way-ahead tied to PPP route analysis that FHWA has funded that will soon commence.</p>
<p>(#201807-9) Confirm the cyber related groups' information is being dispersed through NDTA Primary and Sub committees (Rail/Truck/Ports). [CLOSED]</p>	<p>NDTA</p>	<p>Addressing through the cyber committee and cyber sub-committees to include Fall Meeting cyber committee session for all. Identified in contracts as well as TCJ3 outreach. Challenge for trucking; out of 1.5M motor carriers, SDDC has 800 in network—there are 30-40 are active members and participate.</p>
<p>(#201807-10) Utilize the Port Readiness Committees in future Emergency Deployment Exercises. [CLOSED]</p>	<p>FORSCOM/ SDDC</p>	<p>SDDC CG emphasized the importance of PRCs in multiple forums and by directly contacting USCG leadership and other stakeholders</p>
<p>(#201807-11) Exercise Transportation Priorities and Allocation System (TPAS) Rated Order Contract process {Formerly National Shipping Priority Order (NSPO)/Port Planning Order (PPO)} [CLOSED]</p>	<p>USTRANSCOM/ SDDC/ MARAD</p>	<p>Scheduled 30-31 July 2019 with Port of Tacoma</p>
<p>(#201807-12) Provide guidance for replacement to Qualcomm's tracking/messaging units for TPS shipments. [CLOSED]</p>	<p>SDDC</p>	<p>Actively engaged with NDTA and munitions carriers; last interaction in June '19; received proposal from Boyle Transportation for review.</p>

Attachment 2



Surface EWG Agenda 2019

TOGETHER, WE DELIVER

- **25 July 2019 (0800-1400 hrs) Surface Executive Working Group (Regency, O'Fallon)**
 - **0700-0800 Check In – Refreshments**
 - **0800-0825 Welcome/Introductions [TCDC and Around Room]**
 - **0825-0830 Due Outs Reviewed**
 - **0830-0930 “*State of the Industry*” Trucking, Rail, and Ports**
 - **Break 0930-0945**
 - **0945-1115 Discussion I – Discussion Facilitator: Mr Busler**
Capacity Surge—Equipment, Facilities, and Manpower
 - **1115-1145 Working Lunch**
 - **1145-1330 Discussion II – Discussion Facilitator: Mr Cronin**
Physical and Cyber Intrusions/Attacks; Technology Advances
 - **Break TBD**
 - **1330-1400 *Transportation Management System (TMS)*: Mr Dawson**
 - **1400-1415 Due Outs/Wrap-up/Adjourn**



Motor Carrier Installation Access: The Department's Way-Forward

Date of Update: June 28, 2019

The Department of Defense (DoD) values the role of Motor Carriers in support of our mission, and is committed to improving driver wait times and standard procedures for enabling access to its military installations. The Department continues to enhance and modify procedures and electronic physical access control systems (ePACS) to validate both driver identity and fitness (e.g. active wants/warrants). DoD Manual 5200.08 Volume 3 "Access to DoD Installations" was signed in January 2019, and requires the Services and DoD Agencies to enroll the Transportation Worker Identification Credential (TWIC) and Driver's License in their ePACS, facilitating continuous screening of register drivers and streamlining access on subsequent visits to installations where drivers are registered. The Department is actively working to enhance its ePACS to comply with this new policy.

With the January publication of DoDM 5200.08, Vol III, the Services and DoD Agencies have begun to implement the new policy. Due to mission requirements, physical differences between installations, training, and supporting infrastructure, each installation may have slightly different procedures during, and following implementation. During initial roll out, installations using DBIDS (primarily Air Force, Navy, and Marine Corps) will be able to enroll the TWIC while Army installations will be able to enroll both the TWIC and REAL ID compliant driver's licenses.

Key Elements of New Policy:

Security of DoD installations remains our number one priority. While the new processes are intended to streamline the vetting of the drivers, physical inspections of vehicles remain part of the installation access process.

- DoD installations will implement ePACS, enabling the enrollment process for recurring access.
- The Services are developing, and will soon publish, standardized disqualification criteria, thus eliminating most base-by-base variations.
- Enrolled visitors will undergo a single initial background check by each service. Continuous vetting for new derogatory information will begin upon initial enrollment.
- Once enrolled at an installation, visitors will proceed directly to the appropriate entry control point and have their credential scanned.
- Installations with sensitive missions may restrict access based on security clearance and citizenship.

Attachment 3

Requirements for installation access:

In order to gain access to a military installation (under previous and new policy), the identity, fitness, and purpose of the driver must be verified. Identity is verified using approved credentials – REAL ID compliant driver's license, Transportation Workers Identification Credential (TWIC), or other specified identification.

Fitness is verified in two ways. First, during the initial enrollment process, the visitor control staff will conduct a background check using United States Government criminal records and terrorism databases to ensure that there are no disqualifying offenses. Once enrolled, visitors will be continuously screened for any new derogatory information. If derogatory information is identified during this continuous screening, they will be flagged for further inquiry the next time they access any DoD installation.

The final step in the process is proving purpose for access. Each time a visitor accesses an installation, they are required to provide proof of need to access the installation. Most commonly, in the case of Motor Vehicle Carriers, this will be accomplished with a bill of lading, either paper or electronic. The new policy provides examples of acceptable means of proving purpose but states that the list is not exhaustive. Whenever possible, industry partners are encouraged to provide definitive documentation (paper or electronic) to employees who need to gain access to the installation.

Disqualification:

Under the new policy, the Services will implement common disqualification criteria across all installations. There may be additional criteria for some installations. This criteria will be posted in the visitor centers as well as on installation websites. Installations will also post a redress or appeals process for situations where a visitor believes they have been inappropriately denied access or requires access despite having a disqualifying offense. Please note that some bases require U.S. citizenship, but this is not considered a fitness criteria and so is not standardized across a Service.

Enrollment:

The first time a driver visits an installation under this policy, he or she will be subject to an electronic background check as described above. Once cleared, the visitor's identification credential will be registered with the ePACS and simultaneously registered for ongoing screening. When a visitor returns to the same installation, their same credential will be scanned at the gate and they will be asked their purpose for visiting the installation.

When visiting additional installations, visitors will need to be granted access to the new installation. If they have previously been enrolled in an installation using the same ePACS, their information will be pre-loaded in the system, streamlining the process.

Attachment 3

Current Status:

- All Air Force controlled installations are now enrolling TWICs. Additionally, background checks conducted by other Services are recognized for the initial suitability checks provided that the credential is enrolled in ongoing suitability checks.
- The Defense Logistics Agency has also begun enrolling and recognizing TWICs at their installations. Due to current configuration, initial enrollment must occur at the installation visitor control center rather than truck gates. DLA has requested additional equipment to facilitate registration at truck gates.
- The Army is now register both commercial driver licenses and TWICs.
- The Navy is registering TWICs at the majority of installations and is in the process of revising service level publications to address reciprocal registration recognition.
- The Marine Corps is in the process of revising their policy and will provide an update once approved.
- For installation specific process questions or challenges, the installation access staff at the particular facility is best suited to address industry partner issues.

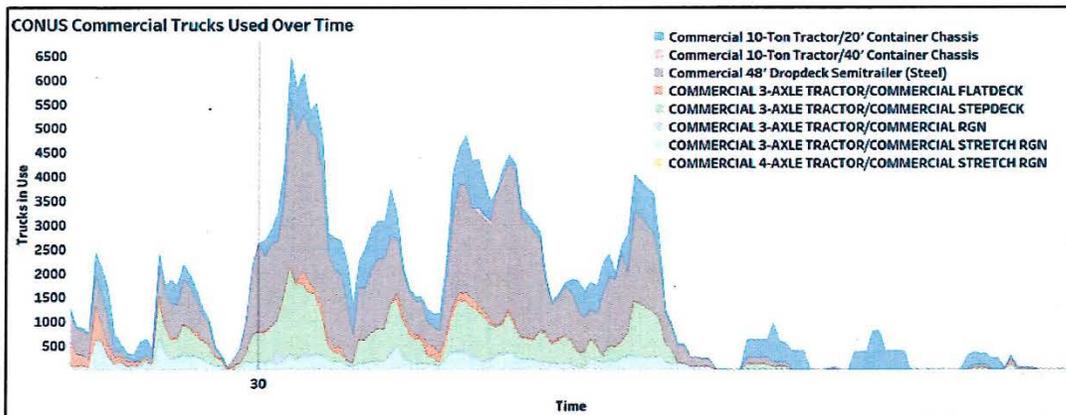
Road Ahead:

- The Department will continue to review policies and procedures to smooth access to installations. As additional installations and services come on-line, this document will be updated.

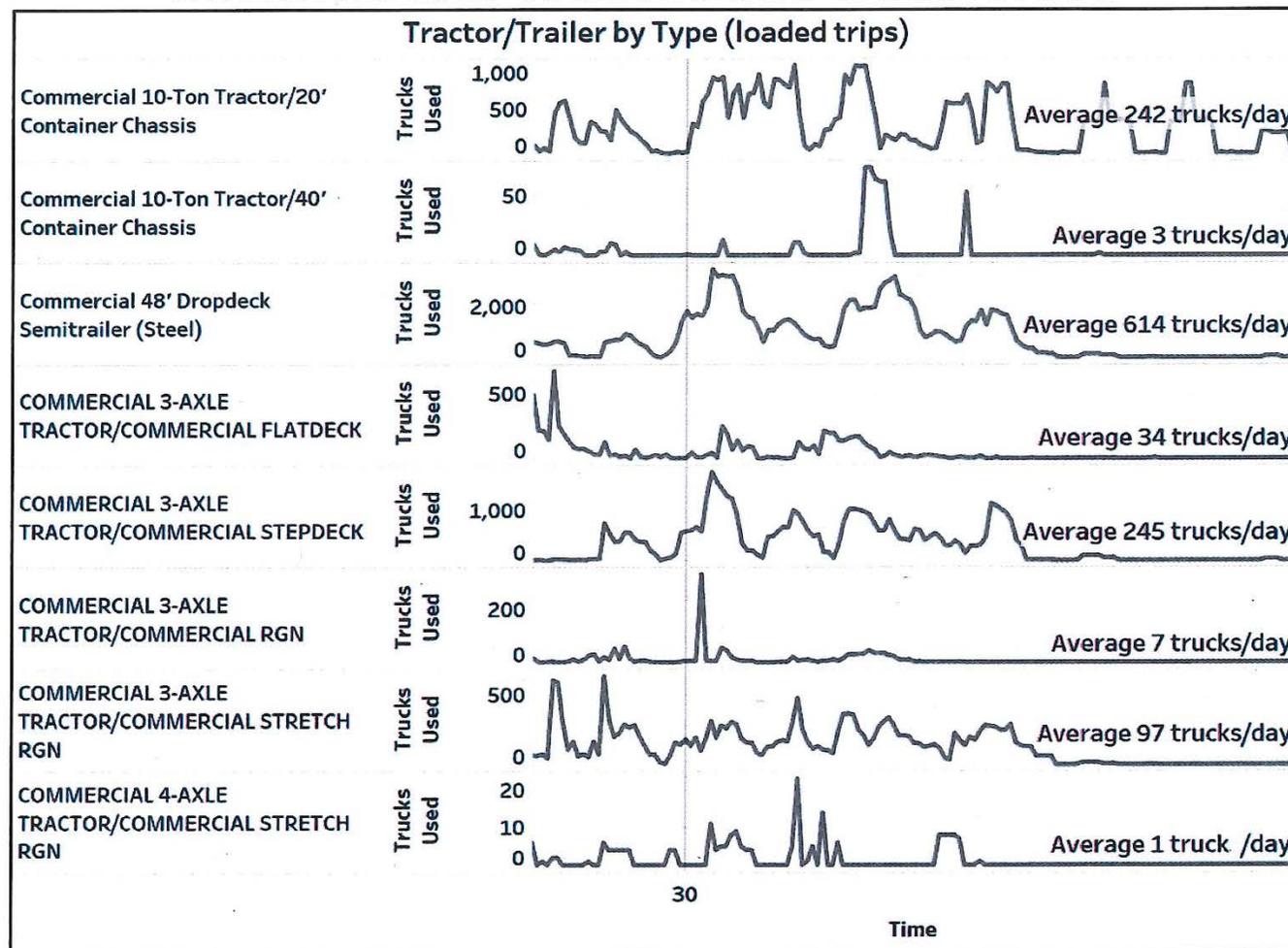
CONUS Commercial Truck Summary

Vital Statistics

- 64,094 pieces/502K Stons moving by commercial truck
- Average of 1,243 truckloads/day moving through CONUS network
- 56,742 offloads
- 2.7M miles traveled
- Peak usage: 6,469 truckloads on day 35
- 1,342 total truckloads on first day of plan



Commercial Truckloads Over Time



Attachment 5

From: [TRANSCOM Scott AFB TCJ3 Mailbox J38 Comm Component](#)
To:

Cc:

Subject: Surface EWG Cyber/Physical Threat Session Follow Up
Date: Monday, August 12, 2019 12:10:34 PM
Attachments: [Cyber Incident Reporting - Unified Message.pdf](#)

Sir/Ma'am –

This email is best viewed in HTML.

This is a follow-up from the 25 July Surface EWG with information you may find useful from the Cyber/Physical Threat discussion portion of the agenda. We have included some organizational and information sharing resources that we hope you find useful.

USTRANSCOM J38 Commercial Industry Branch Information:

Email Address: transcom.scott.tcj3.mbx.j38-comm-component@mail.mil

Information Sharing Website: <https://www.ustranscom.mil/cmd/ciis.cfm>

Branch Phone Number: 618-220-6816

POCs: Ms. Holly Henry, Maj. Chris Moyano, and MAJ Keith Shanklin

USTRANSCOM's Chief Information Security Officer, Mr. Jerry Cronin, pushes out a Cyber Newsletter; if you want to be added to Mr. Cronin's distribution list, please contact him at joseph.g.cronin2.civ@mail.mil.

I have attached a document on cyber incident reporting: Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government.

Ms. Christy Coffey works for the Maritime & Port Security Information Sharing and Analysis Organization (MPS-ISAO). The MPS-ISAO is headquartered at the Global Situational Awareness Center (GSAC) at NASA/Kennedy Space Center, the MPS-ISAO is non-profit, private sector-led, working in collaboration with government to advance Port and Maritime cyber resilience. The core mission is to enable and sustain a safe, secure and resilient Maritime and Port Critical Infrastructure through security situational intelligence, multi-directional information sharing, coordinated response, and best practice adoption supported by role-based education. The MPS-ISAO is a founding member of the International Association of Certified ISAOs (IACI). More information can be found at www.mpsisao.org. Please reach out to her if you wish to discuss her organization's intel sharing information.

Ms. Christy Coffey, EVP Of Operations

Attachment 5

Maritime and Port Security Information and Analysis Organization
469.667.6313 (mobile)
Christy.coffey@mpsisao.org

If you have any questions, please do not hesitate to reach out.

Holly N. Henry
US TRANSCOM
J3/Commercial Industry Branch
DSN 312-770-7961
Team #: 618-220-6816
Comm #: 618-220-7496



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



Attachment 5

systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

Threat Response

Asset Response

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces:

<http://www.fbi.gov/contact-us/field>

Internet Crime Complaint Center (IC3):

<http://www.ic3.gov>

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937
or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):

<http://www.secretservice.gov/contact/field-offices>

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or
<https://www.ice.gov/webform/hsi-tip-form>

HSI Field Offices: <https://www.ice.gov/contact/hsi>

HSI Cyber Crimes Center: <https://www.ice.gov/cyber-crimes>

Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov

United States Computer Emergency Readiness Team:

<http://www.us-cert.gov>

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

If there is an immediate threat to public health or safety, the public should always call 911.