Port of Baltimore, Maryland:

Supply Chain Policy Tabletop Exercise

After Action Report

September 20, 2023

TABLE OF CONTENTS

GENERAL INFORMATION

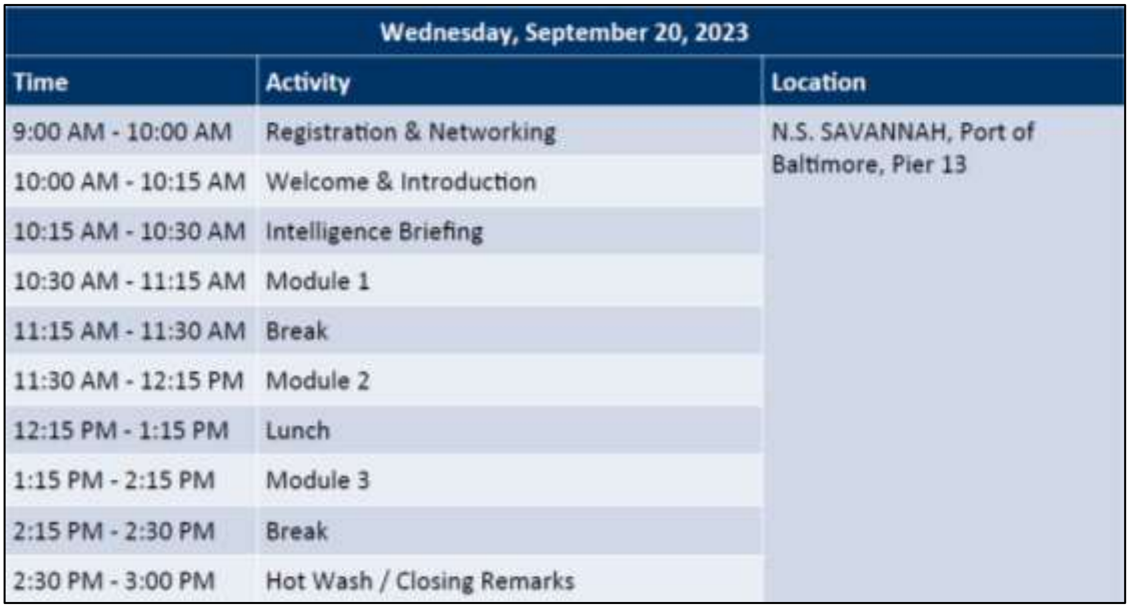
Confidentiality

This was an unclassified exercise. It was suggested that all exercise participants should use appropriate guidelines to ensure proper control of information within their areas of expertise and protect this material in accordance with current directives. Public release of exercise materials to third parties is at the discretion of the exercise planning group.

Exercise Points of Contact

ORGANIZATION
U.S. Committee on the Marine Transportation System
U.S. Army Corps of Engineers

Exercise Agenda



Wednesday, September 20, 2023		
Time	**Activity**	**Location**
9:00 AM - 10:00 AM	Registration & Networking	N.S. SAVANNAH, Port of Baltimore, Pier 13
10:00 AM - 10:15 AM	Welcome & Introduction	
10:15 AM - 10:30 AM	Intelligence Briefing	
10:30 AM - 11:15 AM	Module 1	
11:15 AM - 11:30 AM	Break	
11:30 AM - 12:15 PM	Module 2	
12:15 PM - 1:15 PM	Lunch	
1:15 PM - 2:15 PM	Module 3	
2:15 PM - 2:30 PM	Break	
2:30 PM - 3:00 PM	Hot Wash / Closing Remarks	

U.S. Committee on the Marine Transportation System

The U.S. Committee on the Marine Transportation System (CMTS) serves as a Federal maritime policy interagency coordinating committee for the purpose of assessing the adequacy of the marine transportation system (MTS), promoting the integration of the marine transportation system with other modes of transportation and other uses of the marine environment, and coordinating, improving the coordination of, and making recommendations with regard to Federal policies that impact the marine transportation system. For more information on the CMTS, it's member agencies, and the various teams and working groups please visit https://www.cmts.gov/.

The CMTS Supply Chain and Infrastructure Integrated Action Team focuses on enhancing interagency discussion, communication, and providing recommendations and/or actions in support of the MTS supply chain and facilitating the development of broad evaluation and decision criteria that are used to inform a whole-of-government approach to Federal infrastructure investment in the MTS. The CMTS Supply Chain and Infrastructure Integrated Action Team is the sponsor of this tabletop exercise for the purpose of identifying policies, procedures, and regulations governing the resumption of trade following a supply chain disruption and to identify strategies to mitigate supply chain disruption impacts.

Intermodal Security Training and Exercise Program

The Transportation Security Administration's (TSA) Intermodal Security Training and Exercise Program (I-STEP) provides exercise, training, and security planning tools and services to the transportation community. The program focuses on the security nexus of the intermodal transportation environment, serving mass transit, freight rail, pipeline, port and intermodal, highway and motor carrier, and aviation modes. Working in partnership with the transportation modes, I-STEP enables security partners to:

- Enhance security capabilities – Strengthen plans, policies, and procedures; clarify roles and responsibilities; validate planning needs; and strengthen grant proposals
- Build partnerships – Develop relationships with regional transportation players and other stakeholders.
- Gain insights in transportation security – Network with peers to gain a deeper understanding of security lessons learned and best practices.

I-STEP is the only Federal exercise program to focus on the security nexus of the intermodal transportation environment. As a result, the program reduces risk to individual systems as well as the entire transportation network. I-STEP aligns to TSA's Transportation Systems Sector-Specific Plans (TSSSP) under the National Infrastructure Protection Plan (NIPP). The office of Policy, Plans, and Engagement (PPE) manages this program.

The Exercise Information System (EXIS) portal guides users through a step-by-step exercise planning process to develop their own specific security exercise. EXIS is an intuitive system providing a variety of exercise planning and evaluation tools as well as lessons learned and best practices from the Department of Homeland Security (DHS) Transportation Systems Sector and other aligned user communities. Lessons learned and best practices from exercises and training events along with intelligence information help shape transportation security policy and guidance. Go to: https://exis.tsa.dhs.gov to receive an account and use the tool.

EXERCISE OVERVIEW

Purpose and Scope

The purpose of this exercise was to focus on identifying policies, procedures, and regulations governing the resumption of trade following a supply chain disruption and identify strategies to mitigate supply chain disruption impacts.

Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

For additional information regarding core capabilities, please visit:
https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities.

Exercise Objectives	Capability
Identify federal, state, and local agency and private industry notification processes to MTS disruption supply chain impacts.	• Situational Assessment • Operational Communications • Operational Coordination • Planning
Identify federal, state, and local agency and private industry mitigation roles and responsibilities in response to supply chain disruptions.	• Economic Recovery • Operational Coordination • Critical Transportation • Planning • Logistics and Supply Chain Management
Demonstrate an understanding of the connectivity and interdependencies of surface (road and rail) and maritime transportation systems as they relate to supply chain criticality.	• Supply Chain Integrity and Security • Operational Coordination • Critical Transportation • Logistics and Supply Chain Management
Validate the ability to reroute goods post MTS disruption to mitigate supply chain impacts.	• Supply Chain Integrity and Security • Economic Recovery • Operational Coordination • Planning • Logistics and Supply Chain Management

Table 1. Exercise Objectives and Associated Capabilities

Scenario Overview

The exercise scenarios were designed to assess notification processes, mitigation roles and responsibilities, and the ability to reroute goods in response to supply chain disruptions at the Port of Baltimore, Maryland. Participants engaged in a discussion-based exercise where a major bridge in Baltimore, Maryland collapsed, resulting in a shutdown of portions of the Port of Baltimore. Simultaneously, a Port of Baltimore lessee reported a cyber-attack which caused a complete loss of all containerized cargo information. Participants were then asked to discuss mitigation and response activities seven days post disruption.

Participating Stakeholders

Participating Local, State, and Private Sector Organizations
Canton Railroad
Maryland Port Administration
Maryland Transportation Authority Police
Rutgers University Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) DHS Center of Excellence

Participating Federal Organizations
Bureau of Transportation Statistics
Cybersecurity and Infrastructure Security Agency
DHS Policy – Trade and Economic Security
DOT Office of the Secretary
Federal Highway Administration
Federal Railroad Administration
Maritime Administration
Transport Canada
Transportation Security Administration
U.S. Army Corps of Engineers
U.S. Coast Guard
U.S. Committee on the Marine Transportation System
U.S. Customs and Border Protection
U.S. Department of Agriculture

EXERCISE OUTCOMES

Objective Summary

The exercise outlined four objectives:

1. Identify federal, state, and local agency and private industry notification processes to MTS disruption supply chain impacts.
2. Identify federal, state, and local agency and private industry mitigation roles and responsibilities in response to supply chain disruptions.
3. Demonstrate an understanding of the connectivity and interdependencies of surface (road and rail) and maritime transportation systems as they relate to supply chain criticality.
4. Validate the ability to reroute goods post MTS disruption to mitigate supply chain impacts.

The exercise met the outlined objectives by providing an open, no-fault learning environment wherein capabilities, plans, systems, and processes were discussed and evaluated. Dialog amongst federal, state, and private stakeholders explained steps each agency takes in response to physical and cyber-attacks. Discussions outlined response practices from the agencies and identified gaps in communication and the sharing of sensitive information. Participants identified the need to quantify the aggregate costs of supply chain impacts.

Strengths

- This exercise helped identify MTS policy procedures, capabilities, and gaps that each organization can address.
- Participant cooperation allowed for relationship building amongst stakeholders of various modes of transportation within the MTS. These relationships will ensure a swifter recovery during live events.
- Participants gained better understanding of the represented agencies and their roles and responsibilities, as well as federal requirements within the MTS.
- Participants identified the need for improving networks and cybersecurity coordination.
- If a terminal operating system is offline, paper documents will be used. Carriers and brokers utilize different operating systems and will still be able to access cargo data.
- With the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), all cyber-attacks shall be reported to the Cybersecurity and Infrastructure Security Agency (CISA). Sharing cyber event information with CISA is currently voluntary until final rulemaking. Stakeholders are hopeful this will help streamline reporting and dissemination of vital information without compromising security and sensitive information.

Areas for Improvement

- MTS stakeholders could create an economic impact metric to determine the full impact of a supply chain disruption. The metric could include identifying the aggregate cost of the impact to the supply chain after an incident. The CMTS was identified as a possible champion of this data collection.

- Stakeholders could consider, identify, and utilize a safe and reliable way to share data amongst each other during and after an incident. Exercise discussions identified gaps in data sharing of both non-sensitive and sensitive information. A clear understanding of the chain of command for who shares data, what and when data is shared, and with whom data is shared is vital and should be established prior to an incident.

- Quantitively capture the capability and impact of cargo diversion. Data capture could include the impact on port/terminal throughput, diversion impact to other ports and transportation modes, and impact of associated federal activity, such as U.S. Customs and Border Protection (CBP) redeployment to diverted ports. Data could also include what cargo types may be diverted and to where.

- A need exists for a better understanding of the decision tree (process) of if and when cargo should be diverted. There was a common misconception that the U.S. Coast Guard (USCG) and CBP had this responsibility, where it was discovered the decision of diversion falls on the owner/operator of a vessel.

- Participants identified the need for improving the notification policies and procedures for a cyber event. There were questions regarding what cyber event information should be reported and to whom.

- Follow-on exercises could include additional participants. Organizations identified during the exercise that would have been beneficial for their input to the scenario were the Federal Bureau of Investigation (FBI), Maryland Coordination Analysis Center (MCAC), Transportation Security Operations Center (TSOC), Federal Emergency Management Agency (FEMA), Emergency Support Function (ESF1s), private sector, and other key participants. Future participants could include a representation of the individuals at the "ground level" of these events/incidents.

- Incident reporting requirements on the federal level could be streamlined. When an incident occurs, stakeholders are unsure what to report, when to report, and to whom to report.

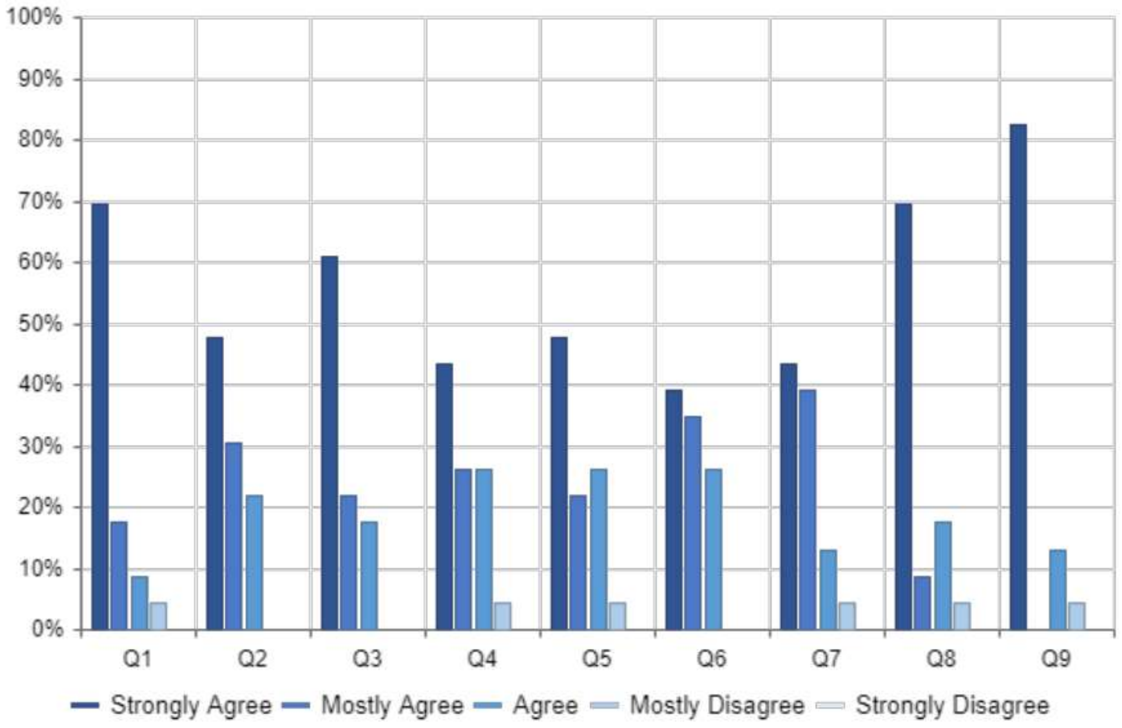
APPENDIX A: PARTICIPANT FEEDBACK

Overview

Forty-seven individuals spanning eighteen agencies/organizations participated in this exercise. All participants had the opportunity to complete feedback forms, which allowed them to provide input on the content and conduct of this exercise. This section includes participants' feedback on the exercise and changes participants would like to implement within their organizations. Feedback questions 1-9 were Likert scale designed, with the results shown below in Table 2 and Figure 1. Feedback questions 10-13 were open-ended survey questions, with the results shown below in Table 3.

#	Question	Strongly Agree	Mostly Agree	Agree	Mostly Disagree	Strongly Disagree
1	The exercise was well-structured and organized.	16	4	2	1	0
2	The exercise scenario was plausible and realistic.	11	7	5	0	0
3	Participation in the exercise was appropriate for someone in my position.	14	5	4	0	0
4	Participants included the right people in terms of level and mix of disciplines.	10	6	6	1	0
5	The exercise was relevant to the risks facing my organization.	11	5	6	1	0
6	The exercise made me aware of new tools, capabilities, and/or resources that will increase my organization's preparedness.	9	8	6	0	0
7	The exercise afforded me the opportunity to network with federal, state, local, tribal, and/or industry stakeholders with whom I did not previously have established relationships.	10	9	3	1	0
8	The exercise was valuable to myself and/or my organization.	16	2	4	1	0
9	I would participate in an I-STEP exercise again.	19	0	3	1	0

Table 2. Likert scale feedback questions. A Likert scale is a rating scale that uses a 5 or 7-point scale that ranges from one extreme attitude to another. It can sometimes be referred to as a satisfaction scale.



Q1: The exercise was well-structured and organized.
Q2: The exercise scenario was plausible and realistic.
Q3: Participation in the exercise was appropriate for someone in my position.
Q4: Participants included the right people in terms of level and mix of disciplines.
Q5: The exercise was relevant to the risks facing my organization.
Q6: The exercise made me aware of new tools, capabilities, and/or resources that will increase my organization's preparedness.
Q7: The exercise afforded me the opportunity to network with federal, state, local, tribal, and/or industry stakeholders with whom I did not previously have established relationships.
Q8: The exercise was valuable to myself and/or my organization.
Q9: I would participate in an I-STEP exercise again.

Figure 1. Likert scale feedback questions in graph form.

10. Of what you learned today, what changes or improvements would you like to implement within your organization?	Improving networks.
	The reports that have been requested from DOD could provide improvement to resiliency, recovery, and contingencies for interruptions to the port, to include the U.S. supply chain.
	Include players that could get vessel agents and the private sector/companies.
	New contacts, better understanding of who owns what.
	Improvements would include more local level participation and more entities. HQ participation by others is higher level and not always representative of what will happen at the ground level.
	Improve cybersecurity coordination.
	Exercise helped to identify policy procedure, capability, gaps that my organization can help address.
	Learned more about other organizations and their role.
11. How do you think the exercise results will assist you in your risk-reduction efforts?	Cooperation and relationship building is key to a swifter recovery when emergent operations occur.
	Helped identify the need for an economic impact metric which the CMTS could possibly assist.
	Understand Federal requirements.
	Will improve creating and coordinating products.
	Points of contact with other modes of transportation.
	Help prioritize follow-on efforts.
	It provided context for what other modes and agencies do in these situations so we can take that into account with the sort of analysis we produce.
	Knowing the operation of each group will help the risk-reduction efforts.
	This is real world. These have happened in my line of work and glad to walk through it in a practice setting.
12. Please comment on any ways future exercises could be improved.	Invite people from Intel Agencies (MCAC/TSOC) that way we can learn from them how the intel is disseminated.
	I will encourage reps from other parts of [my agency] to attend.
	Maybe consider mixing some ICS/FEMA/DOT OST/ESF1s components if applicable.
	Ensure private sector participants to get their reaction to each scenario.
	Invitees should include companies at port and FBI.
	Move participation from economists. Cost to various modes of transportation. Typical commodities that move in and out of the port via rail, road, maritime.
	Really well done, perhaps expand one step further. I.e., past maritime into rail or truck.

13. Please enter additional comments or feedback.	Opportunity to network.
	Very efficient exercise.
	It's a good time length.
	Expectations were met.
	Please try to streamline reporting requirements on Federal level. Our tenants would be able to ID cost lost daily.
	FEMA & trucking participation would have been helpful. Also, DOT RETRAP involvement in the future.
	Explain or provide lists of acronyms.
	It was very well moderated, with a lot of good prompts to keep the discussion flowing without any wasted dead time.
	Outstanding facilitation! Excellent logistics.
	Great venue.

Table 3. Open-ended feedback questions.

APPENDIX B: FULL SCENARIO RECAP

Module 1

On September 20, 2023, at 10:00 a.m., the Port of Baltimore, located in Baltimore, Maryland, receives word from local authorities that the Francis Scott Key Bridge (Key Bridge) experienced a manmade disaster. Multiple media outlets are reporting an explosion occurred on the Key Bridge resulting in a portion of the center span bridge collapsing into the water. The Captain of the Port has set a 500-yard safety zone around the incident area and no vessels may transit under the Key Bridge.

Discussion Questions

1. How is your organization finding out about the bridge collapse?
    a. If you are disseminating information, how and to whom?
    b. Is there any other way information is received by your organization?
        i. How long does it take to receive the information?
    c. USCG sends out information via the alert warning system (AWS). Is your organization signed up to receive these alerts/warnings?
2. How are you personally finding out?
    a. Do you wait for chain of command to inform you?
    b. Do you monitor social media?
        i. Does your agency have members that monitor social media?
3. This incident has occurred and most everyone has said they are pushing out information. Are you redirecting or fueling the questions yourself?
4. How close/far from the incident is the command center located?
5. We know the bridge has collapsed but we don’t know why or what has occurred, does this change anything intelligence-wise or planning if this was or was not a potential terrorist attack?
    a. Would your response actions be for this port only, or for other ports/modes as well?
    b. Is there a particular security / intelligence officer assigned to your organization?
6. When the maritime security (MarSec) level for the port increases, what happens to cargo throughput?
    a. Who has the authority to stop cargo movement?
    b. How is this communicated (phone, email, in-person)?
    c. When MarSec 3 (highest) is reached, what is the USCG immediately telling the Port of Baltimore?
        i. Are there timelines?

ii. Is the MarSec level of other [East Coast] ports increased?

d. With MarSec 3 there is a supply chain impact. Can “we” figure out the cost associated with the impact / delay?

7. If needed, who will tell ships to divert? How quickly?
8. With the vessels stuck in the harbor, what are they doing? Sitting? Offloading?

    a. Are there tugs available 24/ 7/ 365?

    b. Is there a certain threshold coming inbound where a vessel can no longer turn around?

9. Assuming this is a terrorist attack, is there an organization(s) aggregating the economic cost?

    a. Are there economists in your groups?

    i. Are they notified?

10. We know this incident has occurred and we are all receiving information. Who are you relaying information to?

    a. There used to be Maritime Operational Threat Response (MOTR) calls- do these still exist? When are they triggered?

    b. Is there a checklist for notifications?

11. At what level of intel do you disseminate all of this?

    a. Does potential terrorism affect the messaging?

    b. Is there any information you leave out?

    c. Do the public information officers (PIOs) reach out to each other?

    d. Is there a checklist for whom to contact and when?

Module 2

Maryland Port Administration’s Seagirt Marine Terminal is the Port of Baltimore’s container terminal operated by Ports America Chesapeake. On September 20, 2023, at 10:00 a.m., Ports America Chesapeake experienced a cyber-attack which has corrupted their terminal operating system and caused a complete loss of all containerized cargo information.

Discussion Questions

1. We have resources going to the bridge collapse and we also hear about this cyber event, what does this look like for your organization?

    a. What does it change if anything?

2. When the terminal is shut down, how and when does it reopen?
3. Those procedures are all for the movement of goods, what about the cyber security posture?

a. Do you have something in place to conduct a cyber sweep of systems?

4. With reports being made to the National Response Center (NRC), do any organizations not have access to NRC or the information?
   a. Ports America has this incident, how would your organization find out?
5. Is there a requirement to report the cyber incident in the maritime domain?
   a. To whom is the report submitted? When? How?
   b. Where does the information go after it is submitted to NRC?
6. What about a port community information bulletin (PCIB). Does it go out this early?
   a. What is included in the bulletin / alert?
   b. To whom is the bulletin pushed out?
7. If you are forced to use paper for cargo tracking and the terminal is shut down, what capacity would you be at percentage wise to continue cargo movements?
8. It was mentioned about diverting vessel traffic to another terminal. Do we know what that delay cost would be?
   a. Is any agency aggregating this delay cost?
      i. If not, is this something CMTS can look into?
   b. With the East Palestine incident, was an economic assessment completed?
      i. By whom and what were the outcomes?
   c. Is there an assimilated dollar amount associated with the cargo handled by each vessel?
      i. Vessel operating cost of delay(s) and diversion?
9. The undersecretary of policy at DHS wants to set up a supply chain resilience center. With vessels being stuck (anchored) in port, who decides which vessel is first to begin moving again? Is the cargo prioritized?
   a. Are the decisions federally mandated or best practice?
10. Is there a recommended secondary or tertiary location given to vessels for offloading?
    a. Have any studies been completed on the flexibility of terminals to accept diverted vessels?
11. So, this incident / attack occurred here at Seagirt. Do you notify other ports about this incident / attack?
    a. Is there a nexus to tell others? If so, who?

Module 3

Seven days post disruptions, on September 27, 2023, at 10:00 a.m., the Port of Baltimore is still experiencing supply chain impacts as a result of the MTS disruption to the Key Bridge. The 500-yard safety zone around the incident area remains in place and no vessels may transit under the Key Bridge.

Discussion Questions

1. What changes post boom for your organization?
    a. Has MarSec deescalated?
    b. Are there markers for time change?
2. Federal Railroad Administration (FRA): if the company picked another port to offload but cargo still needs to get to Baltimore, how does that work for you?
    a. Are you collaborating with trucking?
    b. Is there a federal law or policy on rail rates?
3. When evaluating the congestion and affects to other modes (rail, road), are there any gaps in information to complete that evaluation?
4. Would the Bay bridge be closed as well?
    a. Would other ports and/or bridges be shut down?

Module 3 Update

It is now 11:15 a.m. on September 27th and things are starting to return to their new normal until the bridge is rebuilt. All organizations and components must begin to look at future planning until the Port of Baltimore returns to operational status.

Discussion Questions

1. The Key Bridge has been rebuilt, what does that change for you?
    a. What are the procedures for vessel movement resumption?
        i. Is there a vessel scoring tool for prioritizing movement?
    b. Would the port look at increasing security afterwards?
2. Has the CMTS gotten involved by this stage? To what point?
3. Are there any changes for the regulatory requirements?
    a. Do facilities need to be reinspected?
4. How would you communicate a back to normal operational status?

Exercise Visual Aids

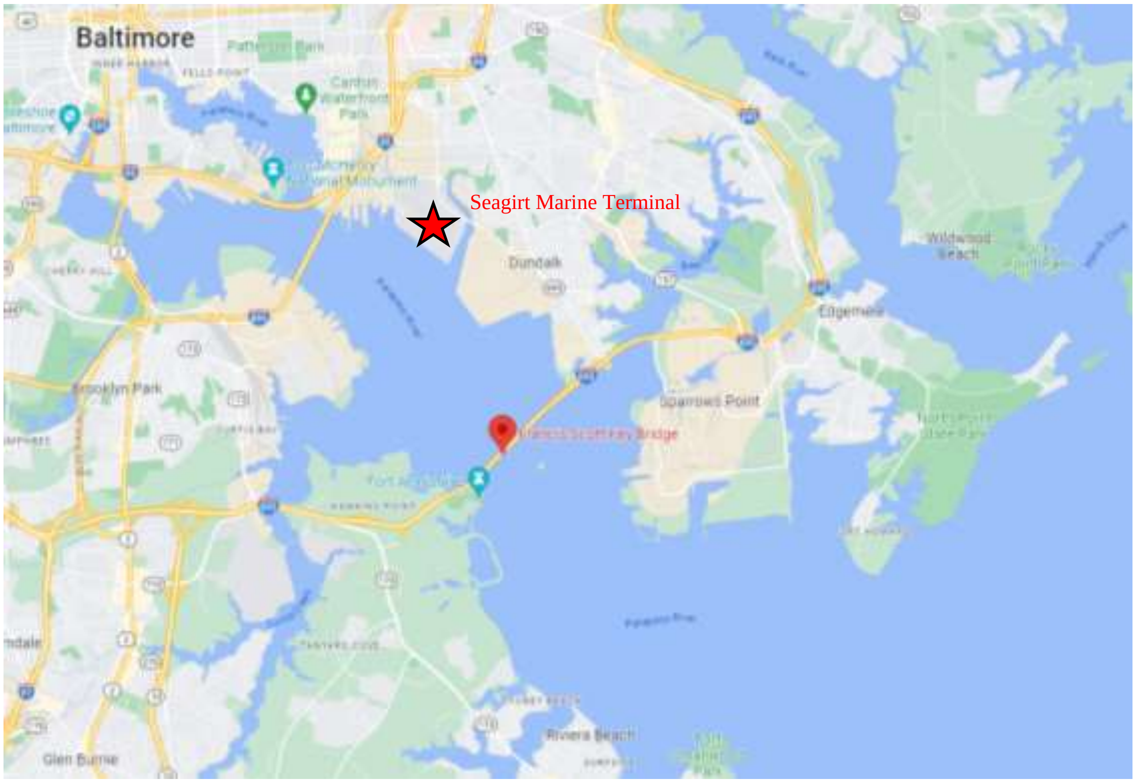


Figure 2. Arial map view of the Key Bridge and Seagirt Marine Terminal, MD

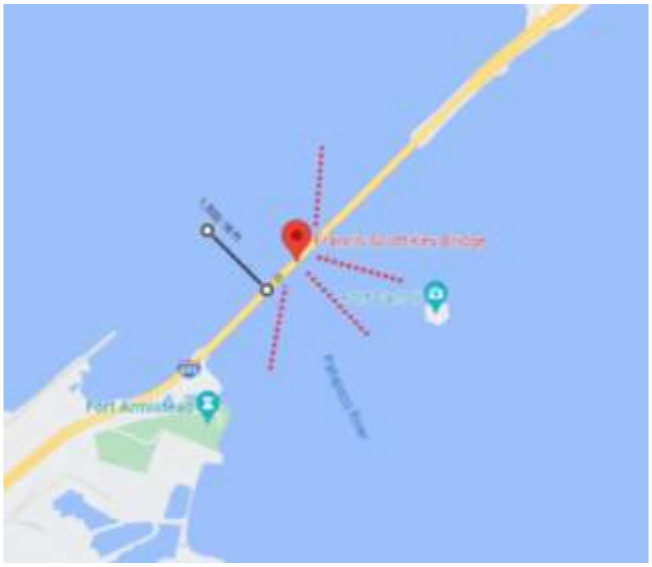
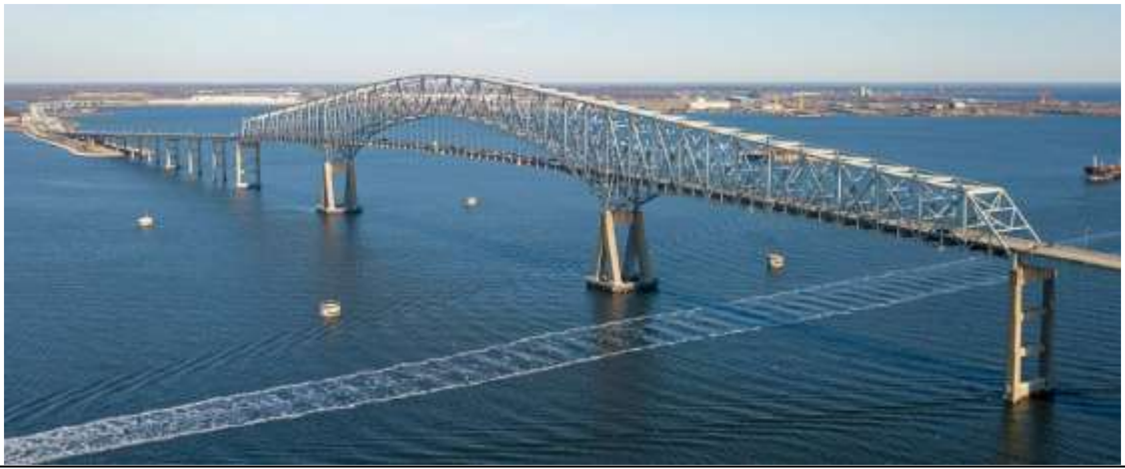


Figure 3. Arial map view of 500-yard safety zone (estimated)



https://en.wikipedia.org/wiki/Francis_Scott_Key_Bridge_%28Baltimore%29#/media/File:Francis_Scott_Key_Bridge_Eastern_View.jpg

Figure 3. Photo view of the Francis Scott Key Bridge, MD

APPENDIX C: PARTICIPANT CONTACT LIST

AGENCY / ORGANIZATION
Canton Railroad
Federal Highway Administration (FHWA)
DOT - Ret Rap
Transportation Security Administration (TSA)
U.S. Committee on the Marine Transportation System (CMTS)
Transportation Security Administration (TSA)
Dept of Transportation
U.S. Coast Guard (USCG)
Customs & Border Protection (CBP)
Cybersecurity & Infrastructure Security Agency (CISA)
Transportation Security Administration (TSA)
U.S. Coast Guard (USCG)
U.S. Army Corps of Engineers (USACE)
Maritime Administration (MARAD)
U.S. Coast Guard (USCG)
Transportation Security Administration (TSA)
Maryland Transportation Authority Police (MDTAP)
U.S. Committee on the Marine Transportation System (CMTS)
Transportation Security Administration (TSA)
Federal Railroad Administration (FRA)
U.S. Coast Guard (USCG)
Maritime Administration (MARAD)
Dept of Homeland Security Policy
Transport Canada
U.S. Committee on the Marine Transportation System (CMTS)
Maritime Administration (MARAD)

Dept of Homeland Security Policy
Transportation Security Administration (TSA)
Transport Canada
Maryland Transportation Authority Police (MDTAP)
Transportation Security Administration (TSA)
Customs & Border Protection (CBP)
Federal Railroad Administration (FRA)
Cybersecurity & Infrastructure Security Agency (CISA)
Federal Railroad Administration (FRA)
Transportation Security Administration (TSA)
Rutgers Univ
Maritime Administration (MARAD)
Maryland Port Administration (MPA)
Customs & Border Protection (CBP)
U.S Dept of Agriculture (USDA)
Transportation Security Administration (TSA)
U.S. Committee on the Marine Transportation System (CMTS)
Transportation Security Administration (TSA)
Customs & Border Protection (CBP)
Maryland Port Administration (MPA)
Dept of Transportation

APPENDIX D: ACRONYMS

Acronym	Term
AAR	After Action Report
AARR	American Association of Railroads
AWS	Alert Warning System
CBP	U.S. Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CMTS	U.S. Committee on the Marine Transportation System
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOT	U.S. Department of Transportation
DOT OST	U.S. Department of Transportation Office of the Secretary
EPT	Exercise Planning Team
ESF	Emergency Support Function
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FRA	Federal Railroad Administration
HQ	Headquarters
ICS	Incident Command System
I-STEP	Intermodal Security Training and Exercise Program
MARAD	Maritime Administration
MarSec	Maritime Security
MCAC	Maryland Coordination Analysis Center
MDOT	Maryland Department of Transportation
MDTAP	Maryland Transportation Authority Police
MEMA	Maryland Emergency Management Agency
MOTR	Maritime Operational Threat Response
MSIB	Marine Safety Information Bulletin

Acronym	Term
MTS	Marine Transportation System
NIPP	National Infrastructure Protection Plan
NRC	National Response Center
PCIB	Port Community Information Bulletin
PIO	Public Information Officer
POC	Point of Contact
PPE	The office of Policy, Plans, and Engagement
SME	Subject Matter Expert
SSI	Sensitive Security Information
TSA	Transportation Security Administration
TSOC	Transportation Security Operations Center
TSSSP	Transportation Systems Sector-Specific Plans
TTX	Tabletop Exercise
USACE	U.S. Army Corps of Engineers
US-CERT	United States Community Emergency Readiness Team
USCG	United States Coast Guard