[Insert Cover Picture]

Maritime Domestic Terror

Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:30am | 9:00am | Welcome and Introductions |
| 9:00am | 9:45am | Module One: Domestic Threat |
| 9:45am | 10:00am | Break |
| 10:00am | 10:45am | Module Two: Domestic Incident |
| 10:45am | 11:00am | Break |
| 11:00am | 11:45am | Module Three: Recovery |
| 11:45am | 12:30pm | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Maritime Domestic Terror Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] and will focus on [insert scope].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, Recovery [select appropriate Mission Areas] |
| **Capabilities** | * Economic Recovery
* Infrastructure Systems
* Intelligence and Information Sharing
* Operational Coordination
* Planning
* Public Information and Warning
* Risk Management for Protection Programs and Activities
* [Select appropriate capabilities]
 |
| **Objectives** | 1. Examine intelligence and information sharing processes, including public messaging protocols, in relation to a credible threat to maritime domestic critical infrastructure.
2. Discuss and identify private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under the National Incident Management System (NIMS) with local, state, and federal agencies.
3. Discuss recovery and business continuity plans in the wake of a maritime domestic terror incident including public messaging protocols.
4. [Insert Additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Vehicle Ramming and Improvised Explosive Device (IED) |
| **Scenario** | An interactive, discussion-based exercise focused on a maritime domestic threat and subsequent domestic terror incident on critical maritime domestic infrastructure.  |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix B.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the 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, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine intelligence and information sharing processes, including public messaging protocols, in relation to a credible threat to maritime domestic critical infrastructure. | * Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
 |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under NIMS with local, state, and federal agencies. | * On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
 |
| Discuss recovery and business continuity plans in the wake of a maritime domestic terror incident including public messaging protocols. | * Economic Recovery
* Infrastructure Systems
* Operational Coordination
* Planning
 |
| [Insert additional objectives as necessary.] | * [Insert capability aligned to each objective]
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players** are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Domestic Threat
* Module Two: Domestic Incident
* Module Three: Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Domestic Threat

## Scenario

### [Insert Incident Date – 6 Days]: 7:15 p.m.

At 7:15 p.m. [insert local time zone], during a routine safety inspection of a small vessel in the [insert nearby body of navigable water], members of the U.S. Coast Guard (USCG) discovered firearms, sophisticated surveillance equipment, and what appeared to be bomb-making materials on board. Coast guard officers immediately apprehended the three individuals on the vessel and turned them over to the Federal Bureau of Investigation (FBI). Upon further examination, investigators found plans and instructional videos for the construction of explosive devices, maps of nearby waterways, photos of several ports, fake transportation worker identification credentials (TWIC Cards), and pre-paid cell phones at the shared residence of the persons on the vessel. Federal authorities released a statement saying they will continue to investigate the apprehended suspects, but there is no evidence of association with other individuals or groups at this time. News outlets throughout the U.S. have begun to report on the incident.

## Discussion Questions

1. How would your organization receive information regarding this incident?
	1. How would your organization receive information about any other threat against domestic maritime facilities?
2. Would your organization access the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal for additional information?
	1. If you do not currently have access to HSIN-CI, are you aware of how to gain access?
	2. What should you expect to see, if anything, on HSIN-CI at this time?
3. How does your organization work with local intelligence and information centers / fusion centers?
4. What types of training does your organization conduct based on general or credible threats?
5. What additional protective security measures can your organization employ at this time?
	1. How do you coordinate protective measures implementation with other organizations within the Transportation Sector?
	2. How do you coordinate protective measures implementation with local, regional, or federal government entities, such as law enforcement agencies, Maritime Administration (MARAD), and your CISA protective security advisor (PSA)?
	3. How does your organization communicate new protective measures to employees?
	4. Are information bulletins and advisories that recommend protective measures that the Department of Homeland Security (DHS) provides useful for your organization?
6. How does your organization share threat information with external stakeholders?
	1. What do they do with this information?
7. How would your actions change if the threat was specific to maritime facilities in your area? Specific to your facility?
8. Are there any other stakeholders outside your organization that you would need to notify based on this information? If so, who?
9. What kind of messaging, if any, would your organization release to the public?

## Scenario Update

### [Insert Incident Date – 4 Days]: 11:15 a.m.

The DHS Office of Intelligence and Analysis (I&A) has reported an uptick in social media threats targeting both private and commercial vessels in and around several U.S. ports and major waterways. They are not, however, able to ascertain a more specific nature of the intended targets, nor the exact goals of the groups. Authorities are currently investigating several domestic extremist groups with ties to international terrorist organizations.

Based on this intelligence, the Secretary of Homeland Security issues an “Elevated” threat alert through the National Terrorism Advisory System (NTAS). In conjunction with DHS, the commandant of the USCG increases the Maritime Security (MARSEC) level to level 2. **(For sample NTAS alert, see Appendix A.)**

## Discussion Questions

1. What information regarding this threat would your organization expect to receive?
	1. What additional information, if any, would you like to receive?
2. How would your organization expect to receive a NTAS alert?
	1. How do you disseminate the alert across your organization?
	2. What would your organization do with this information?
3. What protective security measures or recommendations, if any, will your organization employ following the NTAS Alert?
	1. How would a change in security posture impact your operations?
	2. How long could you maintain heightened security levels until they have an impact on your operations? Why?
	3. How does your organization communicate these protective measures internally?
	4. Do you coordinate protective measure implementation with any other organization within the Transportation Sector, or with government entities, such as law enforcement agencies, the Department of Transportation (DOT), or your CISA PSA?
4. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your personnel?
	1. Who within your organization would receive threat information at this time?
	2. How would your organization disseminate this information internally?
5. What external organizations or individuals would your organization share threat intelligence with at this point?
	1. What notification capabilities (e.g. alerts, emails, telecom, text messages, special tools) do you use to share information and communicate protective measures implementation?
	2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
6. If someone observes identified “suspicious behavior” within your organization, how do your employees report this information locally and within the Transportation Sector?
7. How does your organization monitor trends of suspicious activity across the Transportation Sector nationwide?
8. How has your organization implemented the “If You See Something, Say Something®” campaign or the National Suspicious Activity Reporting (SAR) Initiative?
9. If contacted regarding a threat, what procedures exist at your organization to gather all pertinent information for possible prevention, mitigation of, or recovery from damages because of an attack?
10. Once a threat is received or identified, what procedures exist to immediately engage facility security?
11. At what point, and to what degree, will your organization contact and engage local, state, and federal resources (i.e., local and state law enforcement, fire and rescue, emergency management, and PSA) in response to a credible threat?
12. With whom are you exchanging intelligence and information?
13. What procedures exist to allow emergency on-site access to local rescue and law enforcement personnel?
14. How does your organization integrate your threat and risk management capabilities into your emergency response and recovery plans?

# Module Two: Incident

## Scenario

### [Insert Date]: [Insert Time]

At [insert time], local authorities receive a call from a recreational boater claiming to have seen a [insert type of vessel] that appeared to be heavily loaded down and headed toward [insert major shipping channel / port area]. The boater gives an approximate location of the vessel. Authorities dispatch a USCG craft to investigate.

At [insert time], the sound of an explosion ripping through the [insert shipping channel / port area] shatters daily activities. The suspicious [insert type of vessel] rammed a [insert type of vessel] carrying a small group of people that then exploded. The blast impacted several vessels nearby, many of which were occupied at the time.

Within minutes, [insert location] USCG station and 911 call centers begin to receive mayday calls from individuals around the port who are reporting the explosion and calling for help. Pilots of vessels around the port are frantic, some trying to escape the area and others attempting to approach the scene to rescue victims. Individuals are posting photos and videos of the port on social media. Authorities immediately dispatch rescue vessels and crews with local first responders to assist.

## Discussion Questions

1. How would your organization respond to this incident?
	1. How do your existing emergency operations plans address that response?
	2. What would your immediate priorities be?
	3. Why?
2. Who would you expect to be the first on-scene to respond to this type of incident?
3. How would your organization alert on-duty personnel to this type of incident?
	1. How would you alert off-duty personnel?
	2. Who is responsible for sending out the alert or warning?
4. Do your standard operating procedures (SOPs) include contingency plans in case someone cannot fulfil their roles and responsibilities because of an injury or death?
5. Would your organization deploy additional security personnel as a part of the response to this incident?
	1. How would your organization secure these additional resources?
	2. How will your organization integrate them within your larger response operations?
6. What additional protective measures is your organization considering at this time?
	1. What types of evacuation / shelter-in-place procedures do your organization’s emergency operation procedures (EOPs) include?
	2. Who is responsible for making decisions regarding additional protective measures?
	3. Are local first responders familiar with your emergency procedures?
7. What type of protocols are in place to maintain accountability of your employees during emergency operations?
8. What command and control considerations would responders take at this point in the response?
	1. Would you activate your emergency operations center (EOC)?
	2. Who makes that decision and how would your organization communicate the activation order?
	3. What is the role of private sector stakeholders in this command structure?
	4. Have they trained on incident command procedures?
9. Would fire and emergency medical services personnel use your facility to support rescue operations?
	1. What security considerations would your organization need to make to facilitate that access?
10. How would your organization or business distribute messaging to your employees?
	1. How would you coordinate messaging with any other businesses?
11. Does your organization have an identified public information officer (PIO)?
	1. If so, does your PIO have any experience working with other organization’s PIOs or first responder PIOs?
12. What messaging would you be providing to the media at this time?

## Scenario Update

### [Insert Incident Time + 30 Minutes]

By [insert time], USCG, other rescue vessels, and local first responders are on-scene managing the situation. Responders rescued most of the victims and evacuated them to local hospitals. However, the rammed vessel is severely damaged and sinking. The explosion also caused structural damage to vessels within the vicinity of the incident. At [insert time], the on-scene commander declares rescue operations complete and begins to cordon off the area to contain any potential evidence that law enforcement can use in a subsequent investigation. The captain of the port has closed the port until responders can identify, assess, and mitigate all hazards to navigation.

Initial reports from news outlets are detailing that the blast killed [insert number of people] and [insert number of people] remain in the hospital in various conditions. During a press conference, investigators state that the attackers used [insert number] waterborne IEDs on a [insert type of vessel or vessels] to carry out the attack; the operator(s) of the vessels did not survive.

Investigators, in conjunction with DHS I&A, also report that they are concerned that this attack may be one of a series of attacks planned for the near future. In response, DHS will keep the NTAS level at an “Elevated” status for the next 30 days. In concordance with this, USCG elevates the MARSEC level to level 3 for the next 30 days.

## Discussion Questions

1. What measures would your organization take regarding its overall security posture during and immediately following this incident?
2. How would your organization handle media inquiries?
	1. How quickly is your organization releasing messages to the public?
	2. Who is responsible for this type of messaging?
	3. How is your organization releasing the messaging?
	4. How do different agencies and organizations coordinate messages?
	5. What efforts is your organization taking to address any disinformation that the press may report? What about efforts related to disinformation from social media?
3. How is your organization accounting for on-site personnel?
4. How would a large hazardous materials (HAZMAT) release impact your response priorities and activities?

This page is intentionally left blank.

# Module Three: Recovery

## Scenario

### [Insert Incident Date + Number of Days]:

The explosions resulted in various levels of structural damage to multiple vessels. Responders contained and are mitigating HAZMAT spills and leaks that occurred because of the explosions. There was a total of [insert] fatalities from the attack with an additional [insert] victims sustaining varying levels of injuries. Federal and local law enforcement agencies are continuing their investigations. Your facility has been cleared and is no longer considered a crime scene.

Various news agencies have been analyzing the attacks in [insert location]. The response from the public seems to mainly consist of fear and anger. Social media is rampant with individuals from the region and around the country expressing concern and outrage over government agencies’ inability to prevent the attack. People also seem to be afraid of going back on the water, as local recreational boat rental shops are reporting many cancellations.

In addition, multiple commercial shipping companies have expressed concerns over current security precautions, questioning whether they are enough to prevent an attack on a larger vessel. Several companies have increased their private security in and around their vessels.

Local and federal law enforcement as well as the USCG presence is still high in the maritime areas of [insert location], causing further disruption to businesses and contributing to the reluctance of commercial leisure activities.

## Discussion Questions

1. What are your organization’s priorities following this incident?
2. What are the potential physical / environmental impacts to your operations following an explosion in the water?
	1. Who is responsible for handling physical damages to nearby docks, boats, private property, or land / water wildlife?
	2. How might these recovery considerations impact your organization?
3. What changes would your organization / industry predict as a result of this incident?
4. How could those changes impact your organization’s operations?
	1. How do your existing continuity of operations / business continuity plans address these potentials?
	2. Will these changes affect other transportation sectors (roads, trains, etc.) in the region?
		1. How will they impact those sectors?
		2. How can you manage / mitigate those impacts?
	3. If applicable, how could related changes in the work environment impact labor relations?
		1. Have you engaged local labor representative in your planning process?
5. How will your organization address supply chain issues, both up and down the chain, in the wake of the potential for decreased commercial shipping for an unknown period?
	1. How will the incident impact supply chain goods that you are dependent on, such as fuel and other consumables?
6. How do you determine the operational status of your facilities before, during, and after an incident?
7. What are short-term recovery considerations for your organization or business?
	1. What resources is your organization considering to assist in short-term recovery?
	2. Who is responsible for deciding whether your facility should remain open or close temporarily following an incident?
	3. How does your organization communicate these decisions to the public and the media?
8. Could this incident have an impact on your ability to conduct business?
	1. How could this incident impact your customers and their willingness to do business with you?
9. How do your organization’s EOPs account for handling the spread of potentially erroneous information?
	1. Who is responsible for this?
10. Does your organization or business have employee assistance services (financial, medical, mental health, etc.) available for your employees?
	1. How would your organization communicate available services?
	2. What plans exist to support employees if your facility is unable to open for an extended period?
	3. What if some employees are incapable of returning to work because of the psychological or physical trauma?
	4. Is there an SOP for visitors or outside contractors that the incident impacted?

## Scenario Update

### Date: [Insert Incident Date + Number of Weeks]

Several weeks have passed since the incident. Vessels that had been damaged have been repaired or relocated to a different area so that they can receive the necessary repairs. Any resources that had been lost or re-routed because of the attack have been shipped through alternate means to replenish your resources.

With the facility ready to shift back to normal operating levels, many of your employees are ready to return to work. However, there are some employees and local members of the community who express reservations. Numerous concerns about public safety, safety of your employees, and the long-term impact to the environment from the incident are topics that members of the community and employees wish to address.

## Discussion Questions

1. How could this event impact future operations in the long term (months to years)?
	1. How will your company implement lessons learned during this event to ensure another event such as this does not occur again?
	2. Will your organization share these lessons learned with industry partners and others in the maritime industry to establish best practices and new SOPs to address events such as this?
2. What long-term contingency or continuity of operations plans does your organization have that would apply to this situation?
3. At what point would you consider the area and all associated organizations or businesses stabilized and back to steady state?
	1. Who determines when it is safe for employees, visitors, and outside contractors to return to the area?
4. How would your organization encourage employees to return after such an incident?
5. What could be the cascading effects locally and / or nationally because of a prolonged disruption of your operations?
6. What type of community outreach does your organization have to assure the local community that it is safe to reopen and operate your facility?
7. How would you respond to inquiries from local, state, or federal elected officials?

This page is intentionally left blank.

# APPENDIX A: NTAS Sample Alert

![This image is a sample of a National Terrorism Advisory System Alert. The sample alert reads:   HEADER: National Terrorism Advisory System ALERT Date & Time Issued: [Month] [Day], 20XX   SUMMARY: Based on recent intelligence gathering efforts, the Department of Homeland Security is issuing an Elevated Threat alert for the Maritime Facilities Sector.   DURATION: [Month] [Day], 20XX 12:00 PM - [Month] [Day], 20XX, 11:59 PM  DETAILS:   The Department of Homeland Security in consultation with the U.S. Coast Guard has reviewed newly gathered intelligence and has deemed there to be a credible threat against the maritime facilities sector.   Current intelligence indicates that an attack could be focused on passenger and commercial ships in and around several U.S. ports and major waterways   Authorities are currently investigating several domestic terrorist groups in the United States with ties to international terrorist organizations.   Local law enforcement authorities are encouraged to work with their private sector partners to ensure they are aware of the Elevated Threat status.   AFFECTED AREAS: Current intelligence focuses the threat to both passenger and commercial ships in and around U.S. ports and major waterways.   HOW YOU CAN HELP: The public can assist authorities by reporting any suspicious activity they see. To report suspicious activity, the public should contact their local law enforcement agency and describe specifically what was observed: who or what you saw, when you saw it, where it occurred, and why its suspicious.   BE PREPARED: The public should ensure they are aware of their surroundings in and around U.S. ports and major waterways.   STAY INFORMED: DHS NTAS website: http://www.dhs.gov/alerts and http://twitter.com/NTASAlerts https://dhs.gov/see-something-say-something  FOOTER:  If you see something, say something. Report suspicious activity to local law enforcement or call 911.   The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at www.dhs.gov/alerts. To receive mobile updates: www.twitter.com/NTASAlerts  ]()

This page is intentionally left blank.

1.

# Appendix B: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix C: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **DOT** | Department of Transportation |
| **EOC** | Emergency Operations Center |
| **EOP** | Emergency Operations Procedure |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HAZMAT** | Hazardous Materials |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **I&A** | Intelligence and Analysis |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **MARAD** | Maritime Administration |
| **MARSEC** | Maritime Security |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Reporting |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **TTX** | Tabletop Exercise  |
| **TWIC** | Transportation Worker Identification Credentials |
| **USCG** | United States Coast Guard |

