[Insert Cover Picture]

Multi-Jurisdictional Improvised Explosive Device Bridge Explosion Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all 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 |
| --- | --- | --- |
| 9:00 a.m. | 9:30 a.m. | Welcome and Introductions |
| 9:30 a.m. | 10:30 a.m. | Module One: Pre-Incident Information Sharing |
| 10:30 a.m. | 10:45 a.m. | Break |
| 10:45 a.m. | 11:45 a.m. | Module Two: Incident Response |
| 11:45 a.m. | 12:00 p.m. | Break |
| 12:00 p.m. | 1:00 p.m. | Module Three: Short-Term Recovery |
| 1:00 p.m. | 1:15 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Multi-Jurisdictional Improvised Explosive Device (MJIED) Bridge Explosion 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, and Recovery [Select appropriate Mission Area] |
| **Capabilities** | * Economic Recovery
* Infrastructure Systems
* Intelligence and Information Sharing
* Mass Care Services
* Operational Communication
* Operational Coordination
* Planning
* Risk Management for Protection Programs and Activities
* [Insert additional capabilities as necessary]
 |
| **Objectives** | 1. Evaluate multi-jurisdictional information sharing capabilities and processes among participating organizations responding to a potential threat and then a confirmed improvised explosive device (IED) explosion.
2. Evaluate the ability to establish an effective command structure; provide a safe and secure environment for first responders, law enforcement, and commuters; and provide mass care services during the response to an explosion on [insert bridge name].
3. Examine recovery plans following an attack from an IED with a focus on:
	* Family reunification process
	* Victim assistance
	* Economic and community recovery
4. [Insert additional objectives as necessary]
 |
| **Threat or Hazard** | IED |
| **Scenario** | An interactive, discussion-based exercise focused on a multijurisdictional attack on critical infrastructure. The scenario consists of three modules: Pre-Incident Sharing, Incident Response, and Short-Term Recovery.  |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **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** |
| --- | --- |
| Evaluate multi-jurisdictional information sharing capabilities and processes among participating organizations responding to a potential threat and then a confirmed IED explosion. | * Intelligence and Information Sharing
* Physical Protective Measures
* Planning
* Risk Management for Protection Programs and Activities
* Screening, Search, and Detection
 |
| Evaluate the ability to establish an effective command structure; provide a safe and secure environment for first responders, law enforcement, and commuters; and provide mass care services during the response to an explosion on [insert bridge name] bridge.  | * Intelligence and Information Sharing
* Mass Care Services
* Operational Communications
* Operational Coordination
* Planning
* Risk Management for Protection Programs and Activities
 |
| Examine recovery plans following an attack from an IED, with a focus on: 1. Family reunification process
2. Victim assistance
3. Economic and community recovery
 | * Economic Recovery
* Infrastructure Systems
* Mass Care Services
* Operational Communications
* Operational Coordination
* Planning
 |
| [Insert additional Objectives as needed] | * [Insert additional Capability as needed]
 |

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** 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 the discussion. 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** 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.
* **Data Collectors** 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: Pre-Incident Information Sharing
* Module Two: Incident Response
* Module Three: Short-Term 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 evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page was intentionally left blank.

# Module One: Pre-Incident Information Sharing

## Scenario

## [Insert location]

### [Insert Month, Day, Year]

A domestic violent extremist associated with the Universal Adversary (UA) extremist group posted a video on social media claiming responsibility for an explosion in bus station in [insert city in adjacent state]. In the video, the individual stated, “That was our *warning.”*

The video has since been removed from social media sites; however, it went viral in the three hours it was available. Copies of the video have been re-posted throughout the internet, and there is an increased amount of online chatter from other known members of UA calling for attacks on other U.S. critical transportation infrastructure entities.

Although UA and its associates demonstrate the ability and motivation to carry out an attack, their cause, until now, has been relatively minor and thus ignored. The viral video has earned UA a few moments of mainstream media attention.

Based on this, the Secretary of Homeland Security, in coordination with other federal entities, issues an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible domestic terrorist threat across states in identified areas. There is no information at this time that would warrant the release of an “Imminent” Threat.

The alert is to remain in place until further notice.

## Discussion Questions

1. Would your organization receive information about this potential threat at this time?
	1. How does your organization receive this information?
	2. What would your organization do with this information at this time?
	3. Does your organization participate in intelligence-sharing collaboration efforts specifically regarding critical transportation infrastructure?
2. What steps does your organization take to determine if there is a credible threat?
	1. Who makes this determination on whether there is a credible threat?
	2. How do you triage the information received (formal reporting, rumors, social media etc.) for further dissemination within your organization?
	3. If your organization determines there is a credible threat, what protective measures are put in place? Additionally, who else does your organization contact at this time?
	4. What resources exist or are currently in use to assist you in determining the best course of action in response to this information? (e.g., forums, industry safety bulletins, etc.)
3. Are there processes in place for your organization to share information across the transportation sector with industry partners in other states or regions? If so, what are those processes?
	1. Who are the key stakeholders or groups (e.g., sectors, agencies, associations) with whom you must communicate to protect your critical infrastructure assets?
	2. Is there currently a group (e.g., Information Sharing Working Group [ISWG], Cross Sector Council, regional council, etc.) dedicated to developing information sharing processes?
		1. Can this group be leveraged as a Critical Infrastructure Protection (CIP) governance body?
		2. If not, what alternate structure would be put in place or used for a similar purpose?
	3. Would you share this threat information with international industry partners? What would be the benefit, if any?
4. What resources are used to disseminate information?
	1. What notification capabilities (e.g., alerts, email telecom, short message service [SMS] text, special tools) do you use to share information and communicate protective measures implementation?
	2. Are there measures in place to ensure the security and integrity of the information?
5. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information dissemination?
6. Is your organization aware of suspicious activity reporting (SAR)?
	1. Is SAR training provided within your organization?
	2. What method(s) are used to move the SAR throughout your organization?
	3. Is the information prioritized for immediate referral to the appropriate office or agency for decision or action?
7. Does your organization currently conduct additional hazard / threat specific training?

## Scenario Update

### [Insert Date + 1 Month]

One month later, the Federal Bureau of Investigation (FBI) executes a search warrant in [insert nearby city / town] after receiving notification of an unusually large fertilizer purchase request. During the search, the FBI discovered bomb-making materials in the apartment, along with bomb-making instructional guides that were previously posted on terrorist websites. Two individuals were subsequently arrested and charged.

Additionally, there is evidence that both individuals are in communication with various domestic terrorist organizations throughout the United States and are tied to the individual who posted the viral video. A quick perusal of online forums shows contact and collaboration with at least one known subject in your jurisdiction.

Upon further investigation, law enforcement officials determine that this UA cell is one of an unknown number throughout the area. One of the individuals is demonstrably more dedicated to the UA cause, and a cursory investigation reveals extensive participation in online forums promoting the organization’s cause. Additionally, the FBI discovered a folder with pictures of bridges, overpasses, and major highway junctions on one of the individuals’ laptops. Although positive identification of some locations is possible, there are pictures of structure details that *resemble*, but are not readily identifiable, as the [insert bridge name] in your jurisdiction.

## Discussion Questions

1. Given current and established information sharing procedures, how would this new information change the types of official information distributed to your organization?
	1. How would information from the joint terrorism task force (JTTF) be distributed to your organization?
	2. What information do you expect from government authorities at this point?
	3. What information are you currently expecting from local, state, tribal, or territorial agencies regarding the threat picture or possible response?
2. If you receive information related to potential threats against your facility and personnel first, how would you communicate this information to appropriate entities (e.g., local law enforcement agencies, FBI, your CISA Protective Security Advisor [PSA], etc.)?
	1. What organizations would you communicate with (e.g., local law enforcement agencies, FBI)?
	2. Does your facility maintain a relationship with your CISA PSA? If so, do you have a rapid means of contacting them?
	3. Does your facility use the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) portal?
	4. Is your facility familiar with information sharing documents that are posted on HSIN- CI, such as Joint Intelligence Bulletins (JIBs) or the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) notes?
	5. How is new information integrated into the way you alert those in your organization?
	6. Are there established processes to disseminate threat-related information internally within your company? If so, what are those processes?
3. What plans exist to prevent or deter an attack at your organization?
	1. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance, etc.)?
	2. What physical deterrents does your bridge have in place (e.g., closed-circuit television [CCTV], intrusion detection system [IDS], access control measures)?
	3. Who, or what agencies, control the administration of these deterrents, and who has access to them?
4. How would this potential threat change your organization’s security posture?
5. What actions are local, state, and federal law enforcement agencies taking at this point?
6. What security recommendations, if any, are law enforcement agencies making to private sector stakeholders?
	1. What other information is law enforcement sharing with private sector stakeholders?
7. What type of communication does your organization have with the public at this time?
	1. What information would be shared with your community?
8. Who would take the lead in sharing that information?

# Module Two: Incident Response

## Scenario

### [Insert Month + 2 months, Day, Year]: [Insert time]

Two months pass without any incident. Commuters driving over the [insert name] bridge report a loud noise and feeling the bridge shift and sway. Civilians communicating with 911 indicate several vehicular accidents occurred on the bridge, and there are large amounts of smoke and debris seen coming from underneath the bridge. Several vehicles suffered critical damage from falling debris.

The first law enforcement officers arriving on-scene observe what they believe is severe structural damage to the bridge. There has been a partial collapse of one section of the bridge, and there are fallen cars at the base with possible fatalities inside. They also observe commuters, many of whom are injured and confused, attempting to get out of their cars, and others are trying to drive around stalled and damaged vehicles. Most of the blast and structural damage has occurred approximately halfway across the bridge.

## Discussion Questions

1. How are local law enforcement agencies and first responders contacted?
2. How will local law enforcement and first responders respond to this incident?
	1. How long would it take them to respond to this scene?
	2. In addition to responding to the threat, what other services would they be expected or asked to provide?
3. What other emergency services would respond to this incident?
	1. Since many major bridges are situated between jurisdictions or are subject to shared responsibilities between agencies, what factors determine how responding agencies establish responsibility for the incident?
4. At this time, what other actions would your organization take?
	1. What resources and assets do you have available to assist in the response?
		1. Given the circumstances, would any specialized, heavy rescue equipment or expertise be required?
		2. What specific incident factors will affect the availability and use of specialized equipment or personnel?
5. Is an Incident Command Structure set up at this time?
	1. Who is your organization’s POC?
	2. Who determines immediate command and control?
	3. How are the needs for each requesting agency prioritized?
6. Do your existing plans, policies, and procedures address counter-IED (C-IED) considerations?
	1. Are those plans up to date?
	2. If there are no plans, are you familiar with the free resources available from the CISA Office for Bombing Prevention to assist in incorporating C-IED measures into planning efforts?
7. What safety and security training opportunities relevant to this scenario does your organization provide for employees?
	1. What training resources does your organization leverage from local, state, or federal agencies?
	2. How often does this training take place?
		1. Does the training involve certification, re-certification, or expiration of credentials?
		2. Are your organization’s response capabilities dependent upon updated training, re-certification, or qualified personnel / supervisory personnel being available?
8. How would your organization communicate with groups of people or individuals on the bridge?
	1. Are there any established plans or procedures for this?
	2. What systems are available to assist with this communication?
		1. Will any forms of social media be used to communicate?
	3. Who is responsible for this communication?
9. What are your organizations’ evacuation procedures for an incident of this type?
	1. Who is responsible for activating the evacuation procedures?
	2. How does the potential for additional explosives on-site complicate this response?
	3. Have these evacuation plans been practiced with other responding agencies?
	4. Is there is a specified rally point for evacuees from the bridge?
	5. Would weather impact this location?
	6. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
	7. How might vehicles impacted by the blast affect the evacuation efforts?
	8. What plans or procedures exist to work with those with access and functional needs?
10. What systems, processes, technology platforms, and tools are used to officially share information about the status of the response? Do they facilitate information sharing beyond agency, organization, or jurisdictional lines?
11. Are there technological barriers, polices, legal considerations, or institutional sensitivities that might affect information sharing?
12. For federal, state, or local agencies, what restrictions regarding access to and dissemination of information affect your ability to share information within your organization and with your public and private sector stakeholders (e.g., Protected Critical Infrastructure Information [PCII], sensitive but unclassified [SBU], business critical)?
13. What are the recording / rewriting limits of any present surveillance measures?
	1. Would a review of the footage be retrievable and useable?

## Scenario Update

### [Insert Month, Day, Year]: [Insert time + 30 minutes]

[Insert county / city name] and [Insert state] emergency management agencies release an emergency action notification to [Insert county / city] and surrounding county areas, notifying the public of the current situation.

Despite this, local traffic is backed up for several miles with essential deliveries becoming delayed and alternate routes reaching maximum capacity. Many individuals who abandoned their vehicles on the bridge after the evacuation need transportation.

One officer who is attempting to clear the scene reports numerous red cylinders attached to the bridge support pillars and requests a bomb squad response. Another officer on the scene indicates he’s concerned some of the damaged cars on the bridge might ignite and that fire response could be necessary.

Local news stations are reporting on the explosion at [insert name] bridge. National media outlets are also starting to report on the breaking news stories in the [insert city name] area.

911 is receiving phone calls from families in the area concerned about relatives who commute over the bridge. Operators report that the influx of callers is hampering telecommunications capabilities.

## Discussion Questions

1. What are your organization’s actions at this point?
	1. What resources and assets do you have available to assist in the response?
2. After learning about the numerous red cylinders attached to the bridge support pillars, what impact does this have on your response?
	1. How are your concerns communicated to the responders on and near the bridge?
		1. What considerations / concerns are there regarding signal control around the suspected explosive devices?
	2. What resources are available to you to dedicate to a possible on-scene actor with active control of the explosives?
3. What command structure would be set up for the incident?
4. Which agencies would be involved in unified command?
5. At which point would the emergency operations center (EOC) be stood up?
6. What agencies and organizations will be in the EOC?
7. In addition to unified command, which agencies would have their own command centers set up in other locations?
8. How would arriving state and federal resources integrate into the command structure?
9. Given vehicular access to the site (roadways, restrictions, etc.) who determines the best route to the incident, and which agencies are assigned to any separated areas for the incident?
10. Given the damage, how do you determine which staff are allowed on the bridge at this time to help with evacuation?
	1. What considerations concerning safety, distance, accessibility, and escape routes are being given to the primary and other evacuation sites?
	2. If no one is allowed on the bridge, how does your organization manage accountability of fleeing and injured commuters?
11. Given the questionable integrity of the bridge and the unknown status of the red cylinders, how will arriving emergency medical services (EMS) personnel attend to the injured and casualties?
12. How would resources be coordinated for a mass casualty incident (MCI)?
	1. Who is responsible for that coordination?
	2. What other city / county resources will be used, and how will that occur?
13. What process would first responders have for triaging injuries at the scene?
	1. What resources do first responders need to respond to the potential victims that fell through the bridge?
	2. How would first responders communicate with hospitals and track victims to hospitals?
14. Given the threat of a fire, what actions does your organization take and what other resources might you need to call for?
15. What steps need to take place to ensure the area is cleared of all other potential threats?
	1. How long is it projected to clear the area and ensure there are no secondary devices left?
16. How are surrounding organizations or businesses alerted to the incident?
	1. Who is responsible for this communication?
17. Who is responsible for managing the surrounding traffic?
	1. How many jurisdictions would it involve?
	2. Would it impact any responders for either this incident or other medical emergencies getting to where they need to be?
	3. Given the possible / potential enormity of this event and the allocation of resources, what memorandums of understanding (MOUs) or memorandums of agreement (MOAs) are in place to ensure a proper response to ongoing needs?
	4. At what point is additional assistance requested apart from MOUs / MOAs?
18. Does your organization have a designated Public Information Officer (PIO)? If so:
	1. What protocols exist for alerting partner organizations to an incident?
	2. Who is responsible for sending out the alerts or warnings?
	3. Are there protocols for addressing media inquiries?
	4. How do PIOs receive information from the incident?
	5. Do PIOs have pre-built public information templates for use in different kinds of emergencies?
	6. Would your organization use social media during an incident?
	7. Does your media plan include incidents such as this?
	8. Do you send out any notifications to the public using social media? If so, at what point in the incident would you expect to start sending the notifications?
	9. Have your PIOs had the opportunity to collaborate with other supporting organizations’ PIOs during a crisis?
19. Is a Joint Information Center (JIC) established? If so, at what point in the incident did this occur?
	1. Where would the JIC be located?
	2. Which agencies would be involved?
	3. Would responding agencies coordinate social media messaging?
	4. Is there a location where reporters know to gather when there is an incident?
	5. How are messages coordinated across the different agencies and organizations before the JIC is activated?
	6. Is social media being monitored to maintain awareness of information spreading that may not be accurate?
		1. Who is responsible for mitigating misinformation?
		2. What procedures exist to counter false information on social media?
20. What measures will be taken to streamline the information sharing process?
	1. How will you resolve potential misinformation?
	2. How will you respond to and coordinate any requests for comment from the media?
21. Would you share information with the larger community? How? When?
	1. What would other organizations do with this information?
	2. How would local law enforcement share information with the community?
22. If this were to be declared a terrorist incident, what impact would that have on the response?
	1. How would that determination impact state and federal involvement?
	2. If it were determined that a terrorist organization backed the attacker, as opposed to a lone wolf drawing inspiration from terrorist organization, what impact would that have?

# Module Three: Short-Term Recovery

## Scenario

### [Insert Month, Day, Year]: [Insert Time + 5 hours]

The [insert city name] bomb squad has rendered safe [insert number] suspicious red cylinders found attached to the [insert bridge name] bridge. The bomb squad determined that the red cylinders from the bridge were indeed live IEDs

Law enforcement have secured and evacuated the scene. At this time [insert number] casualties have been identified, including some injured by trampling and panic while escaping the bridge, and an unknown number of people remain missing.

Both 911 and the local and state emergency management agencies continue to receive calls regarding separated and missing family members. Images and videos have gone viral on social media, increasing the strain on emergency response services. Media representatives are now reporting live on-scene and speaking to the public.

Engineers were brought on-site to assess damage to the bridge and report that a full closure is necessary. The projected repair timeline is [insert length of time].

## Discussion Questions

1. What are your organization’s response priorities at this stage of recovery?
2. How are injured patients tracked?
	1. Who is responsible for tracking patients?
	2. What are families of victims being told?
3. What additional resources will be needed for the investigation, crime scene cleanup, and reunion of families with their lost loved ones?
4. How are separated families reunited?
	1. Do you have specific procedures regarding family reunification?
	2. What local facilities and resources can be leveraged for family reunification efforts?
	3. What communication procedures are taking place if people are separated?
		1. How are separated families being contacted?
	4. Is there a specific area for family reunification process?
5. Who is responsible for checking the integrity of the bridge?
	1. Are there contracts in place to bring in professionals to inspect the bridge and determine its safety or necessary repairs?
	2. What impact to the surrounding area is expected with a bridge closure?
	3. With the incident response and priorities growing, how big of a physical area do you foresee your perimeter becoming?
	4. Although it can be considered a low priority, what manpower resources can be spared for perimeter and scene access control?
6. Is social media being monitored to maintain awareness of information spreading that may not be accurate?
	1. Who is responsible for this?
	2. What procedures are in place to counter false information?
7. What additional messaging is being sent out to the local community about the current situation?
8. What communication lines are there between bridge engineers, law enforcement, state government, and transportation services?
9. Are there victim assistance programs in place to assist those the incident impacted?
	1. What does that look like?
	2. Who is responsible for managing victim assistance?
10. Are there mental health services available to assist those the incident impacted?
	1. How would available services be communicated?
	2. How would you respond if some employees are incapable of returning to work because of the psychological or physical trauma?
11. Would family assistance or reunification centers be set up immediately following the incident?
	1. If so, who is responsible for this?
	2. What procedures exist for this?
	3. How are families made aware of where to go?
12. What is the process to collect evidence that belongs to citizens (cell phone video, cameras, security footage from private businesses, etc.)?

## Scenario Update

### [Insert Month, Day, Year]: [Insert Time + 72 hours]

Three days have passed since the attack on [insert bridge name], and the investigation is still ongoing. An additional [insert number] victims were discovered at the base of the bridge in the few cars that fell as a result of the blast. [Insert number] of the previously identified casualties remain hospitalized.

A few days later, traffic around the [insert name] bridge has subsided as commuters find alternate routes around the bridge. However, people parking along the road to visit an impromptu memorial at the scene’s perimeter have resulted in some traffic congestion.

## Discussion Questions

1. How does the command structure change at this point?
	1. How does your organization transfer the investigation over to the FBI?
	2. What responsibilities will your organization have during and after the FBI investigation?
2. What is the expected impact to transportation and industrial sectors from this bridge being closed for the foreseeable future?
3. Considering the impact and potentially international media attention, what measures could be put in place to deter copycat or actual repeated incidents?
4. What would the financial impact be on the area with the bridge being closed because of such an incident?
5. Are there contracts in place to assist in the reconstruction of damaged areas prior to reopening?
6. What plans or contracts with vendors are in place to facilitate clean up after an IED on the bridge?
	1. Who is responsible for coordinating those efforts?
	2. How will the bridge’s structural integrity impact cleanup efforts?
7. While the bridge is closed, who is responsible for managing traffic flow?
	1. How will this diversion of resources impact routine traffic needs?
8. What organization is responsible for the closure of the bridge?
	1. Who will determine when the bridge is safe to return to? How might the return timelines differ for inspectors, cleanup crew, commuters, and other bridge users?
	2. How will they manage to protect the closed bridge from curious bystanders?
9. What would need to happen for the bridge to be back to steady state operations?
10. What local, state, or federal resources are available to assist in recovery or business continuity?
	1. Does [insert name of bridge] have MOUs with local response agencies or other organizations?
	2. What federal and city victim services would be available to those affected?
11. How would memorials be coordinated for those who perished during the attack?
	1. Does the city have any laws restricting the duration or location of memorials?
	2. What control measures are put in place (and when) to keep memorial site attendees / vigils safe during scene security and close enough for their comfort, but outside of your “working” perimeter.
12. Would there be a system to handle donations from the community?
	1. Are there any restrictions regarding donations?
13. What is the plan to handle the significant media attention from national and international outlets?

# Appendix A: 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 B: Maps and Sample Alerts

[Insert relevant maps or alerts used to supplement the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CCTV** | Closed-Circuit Television  |
| **C-IED** | Counter-Improvised Explosive Device |
| **CIP** | Critical Infrastructure Protection |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **EMS** | Emergency Medical Services |
| **FBI** | Federal Bureau of Investigation |
| **HSIN-CI** | Homeland Security Information Network–Critical Infrastructure |
| **I&A** | Office of Intelligence and Analysis |
| **IDS** | Intrusion Detection System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **ISWG** | Information Sharing Working Group |
| **JIB** | Joint Intelligence Bulletin |
| **JIC** | Joint Intelligence Center |
| **JTTF** | Joint Terrorism Task Force |
| **MCI** | Mass Casualty Incident  |
| **MJIED** | Multi-Jurisdictional Improvised Explosive Device |
| **MOA** | Memorandum of Agreement |
| **MOU** | Memorandum of Understanding |
| **NTAS** | National Terrorism Advisory System |
| **PCII** | Protected Critical Infrastructure Information |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Reporting |
| **SBU** | Sensitive but Unclassified |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Experts |
| **SMS** | Short Message Service |
| **TTX** | Tabletop Exercise |
| **UA** | Universal Adversary  |

