Disaster Access Management and Re-Entry 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.

# Acknowledgement

This document incorporates data delivered by Pegasus Research Foundation (PRF) and the National Institute for Hometown Security (NIHS) under DHS Other Transaction Agreement (OTA) No. HSHQDC-07-3-00005. This is not an express or implied endorsement of PRF or NIHS. The Department of Homeland Security is authorized to use, duplicate, release, and disclose data delivered under this OTA in whole or in part, in any manner and for any purposes whatsoever, and to have or permit others to do so. In order to maximize use of this exercise within the emergency management community, the Department authorizes state, local, tribal, and territorial governments and their agents to use, release, and disclose data delivered under the OTA that is contained in this exercise. Please refer any relevant questions to [licensing@cisa.dhs.gov](mailto:licensing@cisa.dhs.gov).

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 7:45 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 10:15 a.m. | Module One: Pre-Incident |
| 10:15 a.m. | 10:30 a.m. | Break |
| 10:30 a.m. | 11:30 a.m. | Module Two: Event + 1–2 Days |
| 11:30 a.m. | 11:45 a.m. | Break |
| 11:45 a.m. | 12:45 p.m. | Module Three: Event + 1–2 Weeks |
| 12:45 p.m. | 1:00 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Disaster Access Management and Re-Entry 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 Areas] |
| **Capabilities** | * Access Control and Identity Verification * Infrastructure Systems * Intelligence and Information Sharing * Operational Communications * Operational Coordination * Planning * [Insert additional capabilities, as necessary] |
| **Objectives** | 1. Discuss access management plans and re-entry procedures with local, state, and federal government agencies and private sector stakeholders. 2. Review intelligence and information sharing processes with local or regional critical infrastructure owners / operators to enable stabilization of community lifelines. 3. Examine recovery and business continuity plans and procedures following a large-scale incident to enable access for critical essential workers. 4. [Insert additional objectives, as necessary] |
| **Threat or Hazard** | Large-scale flooding[[1]](#footnote-1) |
| **Scenario** | Large-scale flooding devastates several local jurisdictions across state lines. |
| **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** |
| --- | --- |
| Discuss emergency action plans and access management and re-entry procedures with local, state, and federal government agencies and private sector stakeholders. | * Access Control and Identify Verification * Intelligence and Information Sharing * Operational Communications * Operational Coordination * Planning |
| Review intelligence and information-sharing processes with local or regional critical infrastructure owners / operators to enable stabilization of community lifelines[[2]](#footnote-2). | * Planning * Infrastructure Systems * Operational Communications * Operational Coordination |
| Examine recovery and information-sharing continuity plans and procedures following a large-scale flooding incident to enable access for critical essential workers. | * Planning * Infrastructure Systems * Operational Communications * Operational Coordination |
| [Insert additional objectives, as necessary.] | * [Insert additional core capabilities as necessary] |

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** 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** 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
* Module Two: Event + 1–2 Days
* Module Three: Event + 1–2 Weeks

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 exercise mission area(s)] 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 exercise mission area(s)] 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 is intentionally left blank.

# Module One: Pre-Incident

## Scenario

## [Insert location]

### [Insert Month, Day, Year]: [Insert time]

[Insert geographic area] storm patterns begin to alarm residents and local government authorities, as the region relies heavily on several local embankment dams and a levee system to store run-off and flood waters from the nearby river and its tributaries. The increase in frequency and severity of recent weather events has some experts worried about the potential for large-scale flooding, which has not occurred in the region for several years.

The National Weather Service (NWS) forecasts light to heavy rain in the region over the next 12-48-hour period and issues a “flood warning.” Residents and other local public and private sector stakeholders start preparing and taking precautions for flooding, as [insert geographic area] is an important economic thoroughfare for shipping and travel. Flooding could disrupt the flow of goods and services for many businesses and communities.

Local governments, along with both public and private sector stakeholders, begin to prepare and coordinate response planning. This situation may hamper the state or local jurisdiction’s ability to control and manage access of key response and recovery resources that can be a critical success factor in enabling community recovery—particularly if the incident affects multiple jurisdictions or involves significant population evacuations.

Consequently, government officials and private sector stakeholders begin to focus on access management considerations in the event of large-scale flooding. As the potential for many nearby jurisdictions to be affected remains high, public-private coordination may be necessary to effectively integrate use of private sector response and recovery assets to stabilize community lifelines, protect critical infrastructure, and restore essential public services to the affected areas.

Although use of access management protocols can enhance disaster management efforts, not all states or jurisdictions have incorporated access management preparedness planning into their emergency operations plans.

## Discussion Questions

1. How will your local or state jurisdiction evaluate the current scenario?
2. How does your state or local jurisdiction coordinate preparedness and response planning with the private sector?
   1. Which local stakeholders and elements of the private sector need to be included in this planning?
   2. Which state or local government official is responsible for developing preemptive response plans and / or coordinating with the private sector?
   3. Will planning focus on public-private coordination to ensure community lifeline stabilization?
   4. Will access management considerations be a part of the planning?
3. What might be some private sector priorities during the development of an access management plan? For example:
   1. Access to facilities and equipment in designated restricted areas or emergency zones pre- or post-emergency to conduct safety shutdown procedures, assess damage, conduct repairs, or stabilize a facility
   2. Designation of critical essential workers or contract carriers, transit routes, escort procedures, and curfew restrictions
   3. Criteria for repopulation, depending on extent of damage and if an evacuation was ordered
4. How will public and community needs be included in the creation of these plans?
5. What difficulties or hurdles does your organization expect to encounter in preparing an access management plan? For example:
   1. List of designated critical infrastructure
   2. Necessary authorities, personnel, or training
   3. Adequate public-private partnerships (P3) or industry POC
6. Does your state or local jurisdiction have a good understanding of potential cascading impacts that can take place during this type of scenario?
7. How will these plans be shared with neighboring jurisdictions and state government officials?
8. What communication channels (formal or informal) does your organization have in place to coordinate with other government and private sector organizations that your operations are dependent upon?
   1. Do you have any pre-identified POCs for those communications in your response plans?
9. What steps will be taken to evaluate the safety of the dams and levees during the pre-incident phase?
   1. How would communities downstream be notified of a potential flood?
   2. What direction would be given to county residents to protect life and property?
   3. How are response operations coordinated with local, state, and federal agencies?
      1. Who is responsible for this coordination?
10. In the event of a flood, what resources does your organization have in place to ensure the security of your facility? Are there any access requirements, gaps, or limitations on employing these resources?
11. How will the media be involved with emergency preparedness?
    1. Who in your organization is responsible for media communications?
12. Does your organization receive alerts from the NWS?

This page is intentionally left blank.

# Module Two: Event + 1–2 Days

## Scenario

## [Insert Location]

**[Insert Month, , DayYear]: [Insert time]**

On the evening of [insert date dependent on regional rainy season], unusually heavy seasonal rainfall for [insert geographic area] continues with yet another large rainstorm. The rainy season has caused the local river, in addition to its many streams and tributaries, to reach flood-stage levels along with producing above average soil moistures. As the latest large rainstorm progresses, the river, streams, and tributaries overflow, creating a massive flood that is quickly approaching the surrounding communities. The seasonal rainfall has also caused several nearby earth-filled embankment dams to be at or near full capacity, resulting in higher than normal water pressure levels on the dams. Small breaches in the embankments at a few of the dams are observed. Following inspection, the dam owners and engineers assess the situation and make the decision to activate their emergency action plans. Through close coordination between the dam owners, engineers, and local emergency management officials, a decision is made to begin evacuation of downstream residents.

Downstream, local media and emergency notification systems hurriedly urge residents to evacuate. A full breach of multiple dams occurs when their already saturated earthen embankments erode, discharging a large volume of water downstream in addition to the water from the flooded streams and tributaries. As a result of the large volume of floodwater, several local levees overtop, compounding the magnitude of the flood event. The large volume of water floods local critcical infrastrucuture, residential areas, and roadways, which affects several communities crossing jurisdictional boundaries.

Emergency dispatchers, first responders, as well as local government officials, are receiving calls and inquiries for information from residents, members of the private sector, and the media. Additionally, people are seeking information from social media, which begins to fill with posts and videos of rushing water and initial damage. Local and national media has mobilized.

However, many people are still frustrated over the lack of information available, including the status of residents, local businesses, and communities the flood has affected. Damage to cell towers and powerlines cuts off internet, electricity, and communications inside the emergency zone. Local senior officials, in coordination with law enforcement, begin to close off roadways into the emergency zone to control incoming traffic.

### [Insert date of event + 24–48 Hours]: [Insert time]

Several dams experienced a complete failure and are retaining no water. The downstream communities are still flooded. Roads that have been rendered impassable because of damage, building debris, and high-water levels have slowed police, fire, and medical personnel response. [Insert state] Governor’s Office of Emergency Services and the Federal Emergency Management Agency (FEMA) are managing logistics and have established a Joint Incident Command Center (JICC).

The governors of [insert affected states] declare a state of emergency and request federal aid and the National Guard. Governmental officials and emergency management staff gather in their respective communities and decide to activate their Emergency Operations Centers (EOC).

Across the region, phone systems, including cellular and 911 are “touch and go” because the functioning communications infrastructure has become overloaded and cell towers have sustained damage from the flooding. State and federal Emergency Support Functions (ESFs) are activated and mobilized, as well as major non-governmental organizations (NGOs).

Emergency management officials, in coordination with law enforcement, have begun to set up access checkpoints, restricting access to designated restricted areas in accordance with their standard operating procedures. Private industries, local business owners, residents, as well as the media and NGOs have attempted to gain access to the emergency zone to determine the status of their businesses and homes, report on the incident, and provide offers of assistance.

In particular, critical infrastructure owners and operators, including the dam owners and engineers, have requested access to the emergency zone to conduct initial damage assessments, protect critical infrastructure, and begin restoration activities. However, checkpoint personnel are unsure which individuals or organizations have been granted access to or through the emergency zone. Therefore, there is a growing need to coordinate access management to assist with response and recovery operations.

Communications across the region remain difficult because of damaged and overloaded cell towers and continuous bad weather. The EOC decidedly establishes alternate methods of communication, and major governmental agencies begin communicating only through hardened channels (e.g., satellite telephones, radio). Most people outside the region of impact are unable to reach their families and friends.

After some time, public works and utility companies are given access to the emergency zone to begin repairs to local communications and power infrastructure. Initial stabilization includes removing downed power lines, shutting off broken water mains, and turning off natural gas service. Stabalization efforts also include clearing debris from roads to allow emergency services to continue response operations and dam and levee personnel to stabilize and begin emergency repairs to their respective breaches.

## Discussion Questions

1. Does your state or local jurisdiction have an access management plan or use private sector re-entry protocols?
   1. Which government officials have the authority to restrict access or approve evacuation, shelter-in-place, or stay-at-home type orders?
   2. Which government officials have the authority to designate access routes, assign escorts to ensure safe passage, or authorize use of drones to assess damage?
   3. What private or public sector organizations or agencies (e.g., federal / state / local government, non-governmental organizations, businesses) would you coordinate with to assist in access management?
   4. How will access plans and procedures be shared and coordinated internally prior to an incident?
   5. Does this plan adequately address the current situation? If not, what issues / questions need to be addressed?
2. Does your organization have a process to communicate your access management plan or re-entry protocols to incident-affected stakeholders?
   1. Who is responsible for communicating and facilitating your access management plan?
   2. How do private sector entities and other incident-affected stakeholders request access?
   3. How are access rules, requirements, and approvals communicated to incident-affected stakeholders?
   4. Who is responsible for collecting and / or approving access requests?
   5. Has your access management plan been coordinated with neighboring states or jurisdictions?
3. Does your state or local jurisdiction issue some type of standardized credential or access token prior to or during emergencies (e.g., access cards, vehicle placards, letters of access [LOA], QR codes)?
   1. Are private sector individuals and organizations able to pre-register (i.e., pre-incident) into your access program?
   2. How will state or local authorities disseminate incident-related access and / or tokens (e.g., electronic or hard copy)?
   3. Who is the approving authority for state or locally issued access credentials and / or access tokens?
   4. What information should be on a government agency or private sector issued LOA?
   5. What secure form of identification or other identifying information should be used with a LOA or other type of access token?
   6. How will this information be shared externally with neighboring states and jurisdictions?
4. How is access management coordinated with local law enforcement and checkpoint personnel?
   1. Who is responsible for coordinating with law enforcement and other checkpoint personnel (e.g., National Guard)?
   2. How are law enforcement or checkpoint personnel notified when access approval has been granted?
   3. How are local law enforcement and other checkpoint personnel informed of approved LOAs or other type of access tokens?
   4. How is deconfliction of access approval or denial conducted?
5. Does your state or local jurisdiction have a formal P3 program or Business Emergency Operations Center (BEOC) capability?
   1. Is your P3 program office or BEOC integrated into your state or local all-hazards emergency operations plan or incident management coordination structures (e.g., EOC, ESF, local emergency planning committee [LEPC])?
   2. Can your P3 program office or BEOC facilitate coordination of private sector access requests?
   3. Is your BEOC virtual and / or only activated during emergencies?
   4. Is your P3 program manager familiar with the FEMA regional Private Sector Liaison and CISA Regional Sector Outreach Coordinator (RSOC)?
6. How will the coordination of “Just-in-Time Access” be communicated to different access checkpoints, law enforcement, and private sector stakeholders?
7. Does your access plan use the access management and phased re-entry approach outlined in the Crisis Event Response and Recovery Access (CERRA) framework to coordinate community lifeline stabilization activities with the private sector? See Figure 1.

|  |
| --- |
| Figure 1 – Example of Phased Re-Entry Process with Access Levels[[3]](#footnote-3) |

**A color-coded chart that defines the “Recommended Phased Re-entry Access Levels.” 

(Row 1, in red) AL-1 – Emergency Response: Emergency zone is unstable – emergency services and authorized support personnel only

(Row 2, in yellow) AL-2 – Response Support: Emergency zone being stabilized – key resources for relief, assessment, stabilization

(Row 3, in green) AL-3 – Recovery Support: emergency zone is stable – support for restoration of community lifelines and essential services

(Row 4, in blue) AL-4 – General Return: Area stable for general re-entry by the public
**

1. What are the protocols your organization’s emergency response plans (e.g., site security plans, emergency occupancy plans, emergency actions plans, or other appropriate plans) have for responding to the incidents described in this module?
2. Has your organization collaborated with other stakeholders to develop contingency plans and processes to maintain safety and security of all personnel and equipment during a severe weather event?
   1. Are local and regional private sector response capabilities integrated into incident management operations?
3. At what stage in the incident would your organization initiate recovery operations?
   1. Who is responsible for making the decision?
   2. What actions has your organization taken to date?
   3. How would / will your organization manage the transition from response to recovery?
4. How does your organization establish priorities for recovery?
   1. What are your priorities at this stage of recovery?
   2. What initial recovery actions would your organization be taking?
5. What roles and responsibilities would your organizational leadership have in this timeframe?
6. How will you coordinate with your various stakeholders, including employees, investors, clients, and / or suppliers?
   1. Do you have a public information officer (PIO)? What is their role?
   2. How would this coordination vary for different types of actions?
7. How are you managing the impacts on your workforce?
   1. Have you identified essential personnel for your core business and essential functions?
8. How are you managing the incident’s impact on your business operations?
   1. Who needs to be informed once normal operations are disrupted? What information needs to be provided? How is this information communicated?
   2. Are you able to maintain operations with alternate work plans (e.g., telework, devolution site, etc.)?
   3. Is your organization considered an essential business and permitted / expected to operate during emergency conditions?
9. How would your organization respond to the temporary loss of communication with transportation personnel (e.g., drivers, operators) or logistical suppliers during the incident? What effect would this have on your supply chain and business continuity?
10. How will you coordinate messaging as the incident continues to evolve?
    1. Who is in charge of coordinating this messaging across communities?
    2. How will rumors and misinformation be addressed?
    3. Is your organization monitoring news or social media to stay aware of what is being reported?
11. How would your organization coordinate with local elected and appointed officials to organize support for stakeholders and other recovery activities?
    1. Who is responsible for that coordination?
    2. What role will the state / local EOCs and BEOC, if established, play in this coordination?
    3. Does your organization have a role in the EOC, BEOC, or an incident-related P3? If so, what role?
12. What steps are you taking as you transition from short-term recovery to intermediate recovery?
13. Does your state or local jurisdiction make use of the CISA guidance on the Essential Critical Infrastructure Workforce?

# Module Three: Event + 1–2 Weeks

## Scenario

## [Insert location]

### [Insert Month, Day, Year]: [Insert time]

Public works and utility personnel, along with first responders, have gradually stabilized the situation in [insert geographic area]. Local communications infrastructure has been repaired, and damaged water mains and gas lines have been rendered secure or are being repaired. Some roadways in the most heavily damaged areas remain impassable as a result of debris or high water. However, major transit routes and bridges have re-opened. Utility and infrastructure personnel are focusing their efforts on re-opening key roadways to allow recovery personnel further, unhindered access into the emergency zone. In addition, the seasonal rain has begun to diminish, and flooding has greatly receded.

Local hospitals have remained open to continue supporting victims of the flood. However, mutual aid agreements between medical facilities did not anticipate a disaster of this scale. Because of the widespread damage and need to restore community lifelines and essential services, displaced residents have taken refuge in Red Cross disaster shelters, local stadiums, and other large facilities at high elevation. Additionally, nearby hotels have taken in a large percentage of displaced residents because of the high demand for temporary shelters. Local authorities have requested aid and additional resources from neighboring jurisdictions, NGOs, and the Federal Government.

Local bus and train stations begin to open, allowing the transportation of personnel, goods, and emergency supplies. Supplies remain limited in quantity but are slowly easing the efforts of local organizations and residents.

## Discussion Questions

1. What information sharing processes would your organization use at this point?
2. How would your organization prioritize recovery efforts?
   1. What are your priorities at this stage of the recovery?
   2. What recovery actions would your organization be taking?
   3. How is private sector and critical infrastructure owners’ subject matter expertise being incorporated into restoration priorities?
3. How would your business maintain operations and continuity in an emergency zone?
4. How would your organization ensure the safety of employees working in an emergency zone?
5. How would your jurisdiction cooperate with private sector entities to ensure critical essential worker access to their facilities within the incident-affected area?
6. What external assets or resources are available to assist your jurisdiction or organization with the overall response effort?
   1. Are pre-arranged agreements in place with any public or private sector organizations to provide resources? Are they formal or informal?
   2. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
   3. How will this coordination and information sharing take place?
7. Would reunification centers or emergency shelters be set up following the incident?
   1. If so, who is responsible for this?
   2. What procedures are in place for this?
8. What roles and responsibilities would your organizational leadership have in this time frame?
9. How are you managing the continued impacts on your workforce and business operations?
   1. How is your organization prepared to operate with manpower shortages?
   2. How is your organization prepared to operate while experiencing supply shortages?
10. How does your agency or organization triage the information you receive (e.g., formal reporting, hearsay, and social media)?
    1. How would a private sector organization or critical essential worker report a denial of movement situation—possibly due to state or local travel restrictions, curfews, etc.?
    2. Has any Essential Critical Infrastructure Workforce guidance been issued?
11. How will you coordinate messaging as the incident continues to evolve?
12. Are there additional notifications that need to be made outside of your organization?

## Scenario Update

## [Insert location]

### [Insert date of incident + 2–4 Weeks]: [Insert time]

As restoration efforts continue for the damaged dams and levee system, the flow of commerce and the return of functioning utilities and essential services has allowed life to return to nearly normal in the least affected areas. The focus of recovery efforts has increasingly shifted to the most devastated areas of [insert geographical areas].

As organizations begin to consolidate their available personnel and resources for redeployment, administrative and manpower burdens begin to ease in the worst affected areas. Additionally, residents originating from less damaged areas begin to return to their homes and businesses. However, many homes in these areas still have water damage and are unfit for occupancy. Residential inspections may be necessary to ensure their adequacy for habitation by returning residents.

While the situation stabilizes, hazardous conditions and further infrastructural damage inside the modified emergency zone limits the ability of response and recovery assets (e.g., utility crews, search and rescue teams, emergency medical personnel) to effectively continue their work. Further cooperation and coordination between all recovery organizations needs to persist to ensure progress.

## Discussion Questions

1. Does your facility or organization have a continuity of operations / business plan for a prolonged incident lasting more than a few weeks?
   1. Does it include a crisis communications plan?
   2. What are the intermediate recovery objectives for your organization?
   3. What are the implications of being unable to open or operate for a period of time?
      1. What would the financial impact be on the facility if a building were closed because of such an incident?
   4. Can your organization move key operations to another location? If so, how long would this take?
2. Given the scenario, are there any additional security measures that your organization would put into place following this incident?
3. What public communications is your organization disseminating?
   1. Who would make decisions regarding the release of information to the public? Who is responsible for distributing public messaging?
   2. How is public messaging coordinated across the relevant stakeholders?
   3. How is your organization coordinating messages with the public sector?
4. What steps are you taking as you transition from intermediate recovery to long-term recovery?
5. What are the long-term recovery objectives for your organization?
6. How will your organization’s priorities shift as residents begin to return to the affected area?
7. Would reunification centers or emergency shelters continue operations?
8. How are you managing the continued impacts on your workforce and business operations?
9. How would you continue to coordinate public messaging?
10. What roles and responsibilities would your organizational leadership have in this time frame?
11. How would your jurisdiction work to formalize access management and re-entry protocols for future incidents?
    1. Will your jurisdiction coordinate preparedness planning and training exercises with neighboring jurisdictions, local government agencies, first responders, or key private sector stakeholders?
    2. Will your jurisdiction consider developing a formal P3 program and / or BEOC to support future events?
    3. Does your organization have formal after-action review meetings? If so, how will private sector comments regarding access management be incorporated?
    4. Will your organization share their best practices and lessons learned with other response organizations, neighboring jurisdictions, and private sector stakeholders?

# 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: Glossary

For the purpose of this document, the following terms and definitions apply[[4]](#footnote-4):

**Access –** Refers to the permission to enter or transit through a geographical area within a jurisdiction that government officials have restricted entry into to maintain public safety or protect property.

**Access Checkpoint –** Refers to the point of access, normally managed by law enforcement, into a restricted area or emergency zone.

**Access Management –** Refers to the process required to coordinate the access or public and private sector response and recovery resources, which may need to enter or transit through designated restricted areas or emergency zones in support of disaster preparation, emergency relief, or restoration efforts.

**Access Program –** Refers to the system or mechanism and the relevant processes and procedures by which a state or local jurisdiction administers access.

**Business Emergency Operations Center –** Refers to an organizational element, sometimes operating in support of a state emergency operations center, intended to share information and coordinate the participation and activities of business, non-profit and volunteer organizations, and private industry partners during disaster management efforts through public-private partnerships.

**Community Lifeline –** Refers to any critical infrastructure sector that provides an indispensable service that enables the continuous operation of critical business and government functions and is critical to human health and safety or economic security[[5]](#footnote-5).

**Emergency –** Refers to any incident, whether natural, technological, or human-caused, that necessitates responsive action to protect life or property.

**Emergency Responder –** Includes federal, state, local, tribal, and territorial government officials, non-governmental organizations, private sector organizations, critical infrastructure owners and operators, and all other organizations and individuals who assume an emergency management role. (Also known as emergency responder)[[6]](#footnote-6).

**Emergency Zone –** Refers to a geographically-defined area that is affected, or is expected to be affected, by an emergency.

**Incident –** An occurrence, natural or manmade, that necessitates a response to protect life or property. In this document, the word “incident” includes planned events as well as emergencies and / or disasters of all kinds and sizes.

**Phased Re-entry[[7]](#footnote-7) –** Refers to the process of managing access and re-entry into a restricted area or emergency zone, in support of response and recovery operations, by categorizing responders and other affected stakeholders into functional groups that may be prioritized for access and re-entry as an incident progresses (e.g., first responders and other incident management personnel, local business owners and utility operators, community members, etc.).

**Restricted Area –** Refers to a geographical area within a jurisdiction in which authorized government officials have restricted access to maintain public safety or protect property.

# Appendix C: Reference List

## CISA Exercises and Resources

* [Critical Infrastructure Exercises](https://www.cisa.gov/critical-infrastructure-exercises)
* [Cybersecurity Training & Exercises](https://www.cisa.gov/cybersecurity-training-exercises)
* [CISA Tabletop Exercise Package (Exercise-in-a-Box)](https://www.cisa.gov/publication/cisa-tabletop-exercise-package)

## Tools

* [CISA Services Catalog, First Edition](https://www.cisa.gov/publication/cisa-services-catalog)

**Active Shooter**

* [Active Shooter Preparedness](https://www.cisa.gov/active-shooter-preparedness)
* [Pathway to Violence Video](https://www.dhs.gov/pathway-violence-video)
* [Pathway to Violence Fact Sheet](https://www.cisa.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf)
* [National Counterterrorism Center (NCTC) First Responder Toolbox](https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox)

**Insider Threat**

* [Insider Threat Fact Sheet](https://www.dhs.gov/publication/fact-sheet-insider-threat-mitigation-program)
* [Insider Threat Mitigation](https://www.dhs.gov/cisa/insider-threat-mitigation)
* [Insider Threat - Training & Awareness](https://www.dhs.gov/cisa/training-awareness)
* [Violence in the Federal Workplace: A Guide for Prevention and Response 2019](https://www.dhs.gov/publication/isc-violence-federal-workplace-guide)

## CISA Architecture

* [CISA’s Cybersecurity Division](https://www.dhs.gov/cisa/cybersecurity-division)
* [CISA’s Emergency Communications Division](https://www.dhs.gov/cisa/emergency-communications-division)
* [CISA’s Federal Protective Service](https://www.dhs.gov/topic/federal-protective-service)
* [CISA’s Infrastructure Security Division](https://www.dhs.gov/cisa/infrastructure-security-division)
* [CISA’s National Risk Management Center](https://www.dhs.gov/cisa/national-risk-management)
* [CISA’s Chemical Facility Anti-Terrorism Standards (CFATS)](https://www.cisa.gov/chemical-facility-anti-terrorism-standards)

## Fact Sheets

* [Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) 1-7: Detection and Delay](https://www.dhs.gov/publication/cfats-detect-delay)
* [Chemical Facility Anti-Terrorism Standards Risk-Based Performance Standards 8 – Cyber](https://www.dhs.gov/publication/cfats-rbps-8-cyber)
* [Chemical Facility Anti-Terrorism Standards Risk-Based Performance Standards 12(iv) - Screening for Terrorist Ties](https://www.cisa.gov/sites/default/files/publications/fs-rbps-12iv-psp-508_1.pdf)
* [Chemical Facility Anti-Terrorism Standards Risk-Based Performance Standards 15 and 16 – Reporting Significant Security Incidents](https://www.dhs.gov/publication/rbps-15-16-incidents-fs)
* [Government Emergency Telecommunications Service (GETS)](https://www.cisa.gov/sites/default/files/publications/GETS%20Factsheet_March%202017%20FINAL%20508C%20031617%20%28003%29.pdf)
* [Homeland Security Information Network — Critical Infrastructure (HSIN—CI)](http://www.dhs.gov/sites/default/files/publications/HSIN-Fact%20Sheet-Critical%20Infrastructure.pdf)
* [If You See Something, Say Something - Information and Public Display Materials](http://www.dhs.gov/see-something-say-something)
* [National Terrorism Advisory System (NTAS) Public Guide, April 2011](https://www.dhs.gov/xlibrary/assets/ntas/ntas-public-guide.pdf)
* [Nationwide Suspicious Activity Reporting Initiative (NSI)](https://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Fact_Sheet_2014.pdf?AspxAutoDetectCookieSupport=1)
* [Protective Security Advisor (PSA) Program](https://www.cisa.gov/sites/default/files/publications/CISA%20Fact%20Sheet%20-%20PSA%20Program%20-%20508c_IAA%20Final.19MAR2020.pdf)
* [Technical Resource for Incident Prevention (TRIPWire)](https://www.cisa.gov/sites/default/files/publications/TRIPwire%20Fact%20Sheet.pdf)
* [Wireless Priority Service (WPS)](https://www.cisa.gov/sites/default/files/publications/Wireless%20Priority%20Service_March%202017_FINAL%20508C%20031617%20%28003%29.pdf)
* Dams Sector Tabletop Exercise Toolkit (DSTET).[[8]](#footnote-8)

## Doctrine and Training

* [Crisis Event Response and Recovery Access (CERRA) Framework, March 2018](https://www.cisa.gov/sites/default/files/publications/Crisis%20Event%20Response%20and%20Recovery%20Access%20%28CERRA%29%20Framework.pdf)
* [CISA Security of Soft Targets and Crowded Places Resource Guide](https://www.dhs.gov/publication/securing-soft-targets-and-crowded-places)
* [Federal Emergency Management Agency (FEMA) – Emergency Management Institute](https://training.fema.gov/emi.aspx)
* [FEMA Independent Study Program](https://training.fema.gov/is/)
* [Security and Awareness Courses](https://training.fema.gov/is/cisr.aspx)
* [Homeland Security Exercise and Evaluation Program (HSEEP), January 2020](https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf)
* [Infrastructure Visualization Platform (IVP) (formerly Computer-Based Assessment Tool (CBAT)](https://www.dhs.gov/infrastructure-visualization-platform)
* [Nationwide Suspicious Activity Reporting Training Courses](https://nsi.ncirc.gov/training_online.aspx)
* [National Infrastructure Protection Plan (NIPP) Overview](https://www.dhs.gov/cisa/national-infrastructure-protection-plan)
* [National Preparedness Goal (NPG), Second Edition, September 2015](https://www.fema.gov/media-library/assets/documents/25959)

## Common Waivers by Event

**Fuel Shortage (Pipeline Release, Prolonged Power Outages) and Mutual Aid / Assistance Efforts**

* [Reformulated Gasoline Requirements (EPA)](https://www.energy.gov/ceser/energy-waiver-library#RFG)
* [Gasoline Reid Vapor Pressure (EPA)](https://www.energy.gov/ceser/energy-waiver-library#GRVP)
* [Federal Motor Carrier Saftey Administration Regulations (DOT)](https://www.energy.gov/ceser/energy-waiver-library#FMSCA)
* [Special Permit (PHMSA)](https://www.energy.gov/ceser/energy-waiver-library#PHMSA)
* [Jones Act](https://www.energy.gov/ceser/energy-waiver-library#JA)
* [Diesel Fuel Penalty (IRS)](https://www.energy.gov/ceser/energy-waiver-library#DFP)

**Severely Impacted Electric Infrastructure**

* [Federal Power Act](https://www.energy.gov/ceser/energy-waiver-library#FPA)

**National Policy Directives and Frameworks**

* [Robert T. Stafford Act (Presidential Declaration)](https://www.energy.gov/ceser/energy-waiver-library#Bob)
* [Presidential Policy Directive – 41 (U.S. Cyber Incident Coordination)](https://www.energy.gov/ceser/energy-waiver-library#PPD)

This page is intentionally left blank.

# Appendix D: Relevant Plans

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

This page is intentionally left blank.

# Appendix E: Relevant Maps / Images

[Insert excerpts from relevant maps or images to be used during the exercise.]

This page is intentionally left blank.

# Appendix F: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **BEOC** | Business Emergency Operations Center |
| **CBAT** | Computer-Based Assesment Tool |
| **CERRA** | Crisis Event Response and Recovery Access |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DSTET** | Dams Sector Tabletop Exercise Toolkit |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **ESF** | Emergency Support Functions |
| **FEMA** | Federal Emergency Management Agency |
| **GETS** | Government Emergency Telecommunications Service |
| **HSEEP** | Homeland Security Exercise and Evaluation Program |
| **HSIN**—**CI** | Homeland Security Information Network—Critical Infrastrucutre |
| **IP** | Improvement Plan |
| **IVP** | Infrastructure Visualization Platform |
| **JICC** | Joint Incident Command Center |
| **LEPC** | Local Emergency Planning Committee |
| **LOA** | Letter of Access |
| **NCTC** | National Counterterrorism Center |
| **NGO** | Non-Governmental Organization |
| **NIHS** | National Institute for Hometown Security |
| **NIPP** | National Infrastructure Protection Plan |
| **NSI** | Nationwide Suspicious Activity Reporting Initiative |
| **NPG** | National Preparedness Goal |
| **NTAS** | National Terrorism Advisory System |

| **Acronym** | **Term** |
| --- | --- |
| **NWS** | National Weather Service |
| **OTA** | Other Transaction Agreement |
| **P3** | Public-Private Partnership |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PRF** | Pegasus Research Foundation |
| **PSA** | Protective Security Advisor |
| **RBPS** | Risk-Based Performance Standards |
| **RSOC** | Regional Sector Outreach Coordinator |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TRIPWire** | Technical Resource for Incident Prevention |
| **TTX** | Tabletop Exercise |
| **WPS** | Wireless Priority Service |



1. While the scenario for this situation manual will focus on a large-scale flooding incident, access management can be applied to any significant incident where state or local authorities need to establish restricted areas or emergency zones to protect public health and safety (e.g., hurricane, wildfire, pandemic, etc.). [↑](#footnote-ref-1)
2. **Community Lifeline** – Refers to any critical infrastructure sector that provides an indispensable service that enables the continuous operation of critical business and government functions and is critical to human health and safety or economic security. For example, the National Response Framework identifies seven community lifelines: Safety and Security; Food, Water, Shelter; Health and Medical; Energy (Power and Fuel); Communications; Transportation; and Hazardous Materials. [↑](#footnote-ref-2)
3. Department of Homeland Security, *Crisis Event Response and Recovery Access (CERRA) Framework*, (Washington, DC: Government Printing Office, 2018), 6, <https://www.dhs.gov/publication/crisis-event-response-and-recovery-access>; For additional information about Phased Re-entry, please see Appendix B: Glossary [↑](#footnote-ref-3)
4. Department of Homeland Security, *Crisis Event Response and Recovery Access (CERRA) Framework,* (Washington, DC: Government Printing Office, 2018), 25-26, <https://www.dhs.gov/publication/crisis-event-response-and-recovery-access>. [↑](#footnote-ref-4)
5. Federal Emergency Management Agency, National Response Framework (Washington, DC: Government Printing Office, 2019), 1, <https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf>. [↑](#footnote-ref-5)
6. Federal Emergency Management Agency, *National Incident Management System,* 2nd ed. (Washington, DC: Government Printing Office, 2008), 139, <https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf>. [↑](#footnote-ref-6)
7. Department of Homeland Security, *Crisis Event Response and Recovery Access (CERRA) Framework,* (Washington, DC: Government Printing Office, 2018), 5-6, 18, https://www.dhs.gov/publication/crisis-event-response-and-recovery-access. [↑](#footnote-ref-7)
8. The Dams Sector Tabletop Exercise Toolbox (DSTET) provides dam owners and operators with exercise planning resources to address sector-specific threats, issues, and concerns related to the protection of dams. For more information please contact the Dams Sector-Specific Agency at [dams@hq.dhs.gov](mailto:dams@hq.dhs.gov). [↑](#footnote-ref-8)