Critical Infrastructure Tabletop Exercise Program

Facilitator / Evaluator Handbook

[Insert Date]

The Facilitator / Evaluator Handbook describes the roles and responsibilities of exercise facilitators and evaluators, and the procedures they should follow. The Handbook is distributed only to those individuals specifically designated as facilitators or evaluators as it contains information about the scenario and exercise administration. It should not be provided to exercise players.

This page is intentionally left blank.

FACILITATOR AND EVALUATOR GUIDANCE

Preparing Exercise Materials

This handbook is a Cybersecurity and Infrastructure Security Agency (CISA) product and a CISA Tabletop Exercise Package (CTEP) document that can be used with all exercise packages included in this program. It is intended to supplement, rather than replace, the Situation Manual (SitMan).

It is recommended that in preparation for exercise conduct, planners compile a facilitator / evaluator packet that includes the Facilitator / Evaluator Handbook, the finalized SitMan, the Exercise Brief Slide Deck, and any relevant background documents.

Facilitators are encouraged to incorporate additional facilitation notes and facilitator questions into the facilitator's version of the SitMan. These facilitator notes and questions are meant to provide the facilitator with additional discussion questions / clarifications that can be used to add substance to an ongoing discussion if necessary.

Facilitating the Exercise

During the exercise the facilitator is responsible for keeping participant discussions on track with exercise objectives and ensuring all issues and objectives are explored as thoroughly as possible within time constraints. If an exercise uses breakout groups, more than one facilitator may be needed. The facilitator generally presents the multimedia briefing, which describes the scenario and any relevant background information. The facilitator also leads the discussion, introduces spokespersons, poses questions to the audience, and ensures that the schedule remains on track. A good facilitator should possess:

- The ability to keep side conversations to a minimum, keep discussions on track and within established time limits, control group dynamics and strong personalities, and speak competently and confidently about the subject without dominating conversation;
- Functional area expertise or experience;
- Awareness of appropriate plans and procedures; and
- The ability to listen well and summarize player discussions.

If feasible and/or appropriate, co-facilitators who are knowledgeable about local issues, plans, and procedures may assist the lead facilitator. Also, designating a recorder to take notes allows the facilitator to focus on key discussion issues. During the exercise, the facilitator helps evaluators collect useful data by keeping discussions focused on exercise objectives and core capabilities.

Observing and Evaluating the Exercise

Evaluators / data collectors must keep an accurate written record of the discussion and what occurs. They should take notes as players discuss actions, make decisions, and present their capabilities. Notes should identify the following:

- *Who* (by name or position) made the decision?
- *What* occurred (the observed decision)?
- *Why* the decision was made (the trigger)?
- *How* did they make the decision (the process)?
- *What* were the outcomes of each decision? Was a solution identified? Who is responsible for the identified solution? In what time frame will the solution be completed?

Tips for Successful Evaluation

DO:
- Focus on plans, policies, and procedures
- Take detailed notes
- Write legibly

DO NOT:
- Prompt players
- Get in the way
- Answer questions for players (refer questions to the facilitator)

Effective notes will assist when writing the final analysis. During the exercise, it is important to concentrate on recording what is happening, specifically, what is discussed by the group as it relates to the exercise objectives and capabilities identified. Lengthy and detailed writing during the exercise can cause evaluators / data collectors to miss important discussions among participants, so it is important to focus on points relating to the exercise objectives.

Identifying the key events makes recording the action manageable, eliminates unnecessary information, and provides the kind of data most useful for the after action process.

Items and issues to be aware of during the discussion include:

- Existing plans or procedures that will help the agency / group / jurisdiction / organization achieve the stated exercise objectives and demonstrate the appropriate capability(ies).
- Deviations from those plans and implementation procedures.
- Roles and responsibilities of players with actions and decisions related to the exercise objectives and capabilities (if applicable).
- Decisions made by exercise players.
- Recommendations offered by players.
- Any unresolved issues discussed during the exercise.

Hot Wash

Immediately after the exercise, a hot wash will be conducted with the players and facilitators. A hot wash allows players the ability for self-assessment and discussion on their performance in the exercise. The hot wash should address the following questions:

- Were the exercise objectives met? Why or why not?
- What are the major positive items or achievements that were identified during the exercise?
- What are the major gaps or deficiencies that need to be addressed?

- What other additional issues need to be addressed?
- What are the next steps for addressing the gaps or deficiencies both short and long term?
- What did you get out of this exercise?

The hot wash also provides the evaluators / data collectors with the opportunity to clarify points or collect any missing information from the players before they leave the area. To supplement the information collected during the player hot wash, the evaluation team distributes participant feedback forms to get responses from participants based on their perception of the exercise.

Facilitator and Evaluator Debriefing

Following the hot wash, facilitators and evaluators / data collectors should conduct their own debriefing to reconcile conflicting outcomes and solidify common themes. At the debriefing, facilitators and evaluators / data collectors will further discuss the performance of the exercise participants. In addition, facilitators and evaluators / data collectors should provide what they thought were three strengths and three areas for improvement observed during the exercise. This is often referred to as "three ups" and "three downs." These strengths and areas for improvement are based on general feedback from the facilitators and evaluators / data collectors immediately after the exercise and should be relevant to the selected capabilities.

Analyze Data

The goal of data analysis is to assess performance by identifying key exercise strengths and areas for improvement. The analysis compares players' discussions with existing plans and procedures. Data analysis includes:

1. Review of exercise discussion notes
2. Comparison of player discussions to existing plans
3. Identification and explanation of deviations
4. List of recommendations to resolve issues

During data analysis, the evaluator / data collector consolidates data collected during the exercise and transforms it into narratives that address the course of exercise play, demonstrated strengths, and areas for improvement.

A template for an exercise write-up (and analysis of the identified issues) is provided in **Appendix B.**

Identify Root Causes and Develop Recommendations

To produce an After-Action Report / Improvement Plan (AAR / IP) with recommendations for improving preparedness capabilities, it is critical for evaluators / data collectors to discover not only what happened, but why events happened or certain decisions occurred. Evaluators / data collectors must find the root cause for each objective not completed as expected. A root cause is the source of, or underlying reason behind, an identified issue (as uncovered during analysis) toward which the evaluator / data collector can direct an improvement. To arrive at a root cause, an evaluator / data collector should attempt to trace each event back to its origin. Root cause

analysis may require the review and evaluation of emergency plans, training programs, policies, and procedures.

Uncovering root causes enables the development of actionable solutions for improvement areas identified in the AAR / IP. These recommendations are based on the evaluator or evaluation team's experience and best judgment, although the responsibility for implementing recommendations ultimately lies with the leaders and managers of the participating organizations or agencies.

Evaluators / data collectors should use the following questions as a guide for developing recommendations for improvement:

- Were the objectives of the exercise met?
- Did the discussion suggest that all personnel would be able to successfully complete the tasks necessary to execute the activity? If not, why?
- What are the key decisions associated with each activity?
- Did the discussion suggest that all personnel are adequately trained to complete the activities / tasks needed to demonstrate the capability?
- Did the discussion identify any resource shortcomings that could inhibit the ability to execute an activity?
- Do the current plans, policies, and procedures support the performance of activities? Are players familiar with these documents?
- Do personnel from multiple agencies, jurisdictions, or organizations need to work together to perform a task, activity, or capability? If so, are there agreements or relationships in place to support the coordination required?
- What was learned from this exercise?
- What strengths were identified for each activity?
- What areas for improvement are recommended for each activity, if any?

Identify Lessons Learned

For the purposes of the Homeland Security Exercise and Evaluation Program (HSEEP), a *lesson learned* is knowledge and experience (both positive and negative) derived from observations and historical study of actual operations, training, and exercises. Lessons learned provide valuable insight on how to approach similar concerns in the future. A lesson learned is not only a summary of what did or did not go wrong; it provides information that may later be relevant. Consider if there are lessons learned worth sharing and recommend them for approval from appropriate organizational authorities.

Example of a Lesson Learned:

"During a chemical weapons exercise, the jurisdiction found that using buses to transport large numbers of walking wounded to medical facilities improved incident response by reducing strain on EMS vehicles and by decreasing transit times for victims. This lesson learned involved a number of agencies and disciplines and can be widely applied."

After-Action Report and Improvement Plan

An After-Action Report/Improvement Plan (AAR / IP) is used to provide feedback to participating entities on their performance during the exercise. The AAR summarizes exercise events and analyzes performance by identifying key exercise strengths and areas for improvement. It also evaluates achievement of the selected exercise objectives and the demonstration of the overall capabilities being validated. The IP portion of the document includes corrective actions to take to improve performance, along with timelines for their implementation, and assignment to responsible parties.

The lead exercise planner or evaluator must determine when exercise write-ups are due and ensure the evaluators / data collectors are given a "**no later than date,"** for submission. It is strongly recommended that the AAR / IP utilize the HSEEP AAR / IP template.

An abundance of data is captured by each evaluator / data collector and this information is consolidated to produce the AAR / IP. The evaluators / data collectors should review the sample AAR / IP write-up located in **Appendix B**.

This page is intentionally left blank.

APPENDIX A: CORE CAPABILITIES[1]

The following excerpts are taken from the U.S. Department of Homeland Security's National Preparedness Goal, September 2015.

Planning (All Mission Areas)

Definition: Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Preliminary Target:

1. Identify critical objectives during the planning process, provide a complete and integrated picture of the sequence and scope of the tasks to achieve the objectives, and ensure the objectives are implementable within the time frame contemplated within the plan using available resources for prevention-related plans. (Prevention)[1]
2. Develop and execute appropriate courses of action in coordination with local, State, tribal, territorial, Federal, and private sector entities in order to prevent an imminent terrorist attack within the United States. (Prevention)
3. Develop protection plans that identify critical objectives based on planning requirements, provide a complete and integrated picture of the sequence and scope of the tasks to achieve the planning objectives, and implement planning requirements within the time frame contemplated within the plan using available resources for protection-related plans. (Protection)
4. Implement, exercise, and maintain plans to ensure continuity of operations. (Protection)
5. Develop approved hazard mitigation plans that address relevant threats / hazards in accordance with the results of their risk assessment within all local, State, tribal, territorial, and Federal partners. (Mitigation)
6. Develop operational plans that adequately identify critical objectives based on the planning requirement, provide a complete and integrated picture of the sequence and scope of the tasks to achieve the objectives, and are implementable within the time frame contemplated in the plan using available resources. (Response)
7. Convene the core of an inclusive planning team (identified pre-disaster), which will oversee disaster recovery planning. (Recovery)
8. Complete an initial recovery plan that provides an overall strategy and timeline, addresses all core capabilities, and integrates socioeconomic, demographic, accessibility, technology, and risk assessment considerations (including projected climate change

[1] This document was last updated 11/4/2016. All Core Capabilities, Definitions, and Preliminary Targets were copied from the:

- FEMA Website: https://www.fema.gov/core-capabilities; accessed 11/4/2016
- National Preparedness Goal, Second Edition, September 2015

[1] Specific mission area added only for those core capabilities which cover more than one mission area.

impacts), which will be implemented in accordance with the timeline contained in the plan. (Recovery)

Public Information and Warning (All Mission Areas)

Definition: Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard, as well as the actions being taken and the assistance being made available, as appropriate.

Preliminary Target:

1. Share prompt and actionable messages, to include National Terrorism Advisory System alerts, with the public and other stakeholders, as appropriate, to aid in the prevention of imminent or follow-on terrorist attacks, consistent with the timelines specified by existing processes and protocols. (Prevention)
2. Provide public awareness information to inform the general public on how to identify and provide terrorism-related information to the appropriate law enforcement authorities, thereby enabling the public to act as a force multiplier in the prevention of imminent or follow-on acts of terrorism. (Prevention)
3. Use effective and accessible indication and warning systems to communicate significant hazards to involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets). (Protection)
4. Communicate appropriate information, in an accessible manner, on the risks faced within a community after the conduct of a risk assessment. (Mitigation)
5. Inform all affected segments of society by all means necessary, including accessible tools, of critical lifesaving and life-sustaining information to expedite the delivery of emergency services and aid the public to take protective actions. (Response)
6. Deliver credible and actionable messages to inform ongoing emergency services and the public about protective measures and other life-sustaining actions and facilitate the transition to recovery. (Response)
7. Reach all populations within the community with effective actionable recovery-related public information messaging and communications that are accessible to people with disabilities and people with limited English proficiency, protect the health and safety of the affected population, help manage expectations, and ensure stakeholders have a clear understanding of available assistance and their roles and responsibilities. (Recovery)
8. Support affected populations and stakeholders with a system that provides appropriate, current information about any continued assistance, steady state resources for long-term impacts, and monitoring programs in an effective and accessible manner. (Recovery)

Operational Coordination (All Mission Areas)

Definition: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Preliminary Target:

1. Execute operations with functional and integrated communications among appropriate entities to prevent initial or follow-on terrorist attacks within the United States in accordance with established protocols. (Prevention)
2. Establish and maintain partnership structures among Protection elements to support networking, planning, and coordination. (Protection)
3. Establish protocols to integrate mitigation data elements in support of operations with local, state, tribal, territorial, and insular area partners and in coordination with Federal agencies. (Mitigation)
4. Mobilize all critical resources and establish command, control, and coordination structures within the affected community and other coordinating bodies in surrounding communities and across the Nation and maintain as needed throughout the duration of an incident. (Response)
5. 2. Enhance and maintain command, control, and coordination structures, consistent with the National Incident Management System (NIMS), to meet basic human needs, stabilize the incident, and transition to recovery. (Response)
6. Establish tiered, integrated leadership, and inclusive coordinating organizations that operate with a unity of effort and are supported by sufficient assessment and analysis to provide defined structure and decision-making processes for recovery activities. (Recovery)
7. Define the path and timeline for recovery leadership to achieve the jurisdiction's objectives that effectively coordinates and uses appropriate local, State, tribal, territorial, insular area, and Federal assistance, as well as nongovernmental and private sector resources. This plan is to be implemented within the established timeline. (Recovery)

Intelligence and Information Sharing (Prevention, Protection)

Definition: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction (WMDs); or any other matter bearing on U.S. national or homeland security by local, State, tribal, territorial, Federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Preliminary Target:

1. Anticipate and identify emerging and/or imminent threats through the intelligence cycle. (Prevention)
2. Share relevant, timely, and actionable information and analysis with local, State, tribal, territorial, Federal, private sector, and international partners and develop and disseminate appropriate classified / unclassified products. (Prevention)

3. Ensure local, State, tribal, territorial, Federal, and private sector partners possess or have access to a mechanism to submit terrorism-related information and/or suspicious activity reports to law enforcement. (Prevention)
4. Anticipate and identify emerging and/or imminent threats through the intelligence cycle. (Protection)
5. Share relevant, timely, and actionable information and analysis with local, State, tribal, territorial, Federal, private sector, and international partners and develop and disseminate appropriate classified / unclassified products. (Protection)
6. Provide local, State, tribal, territorial, Federal, and private sector partners with or access to a mechanism to submit terrorism-related information and/or suspicious activity reports to law enforcement. (Protection)

Interdiction and Disruption (Prevention, Protection)

Definition: Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

Preliminary Target:

1. Maximize our ability to interdict specific conveyances, cargo, and persons associated with an imminent terrorist threat or act in the land, air, and maritime domains to prevent entry into the United States or to prevent an incident from occurring in the Nation. (Prevention)
2. Conduct operations to render safe and dispose of chemical, biological, radiological, nuclear, and explosive (CBRNE) hazards in multiple locations and in all environments, consistent with established protocols. (Prevention)
3. Prevent terrorism financial / material support from reaching its target, consistent with established protocols. (Prevention)
4. Prevent terrorist acquisition of and the transfer of CBRNE materials, precursors, and related technology, consistent with established protocols. (Prevention)
5. Conduct tactical counterterrorism operations in multiple locations and in all environments, consistent with established protocols. (Prevention)
6. Deter, detect, interdict, and protect against domestic and transnational criminal and terrorist activities that threaten the security of the homeland across key operational activities and critical infrastructure sectors. (Protection)
7. Intercept the malicious movement and acquisition / transfer of CBRNE materials and related technologies. (Protection)

Screening, Search, and Detection (Prevention, Protection)

Definition: Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

Preliminary Target:

1. Maximize the screening of targeted cargo, conveyances, mail, baggage, and people associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means. (Prevention)
2. Initiate operations immediately to locate persons and networks associated with an imminent terrorist threat or act. (Prevention)
3. Conduct CBRNE search / detection operations in multiple locations and in all environments, consistent with established protocols. (Prevention)
4. Screen cargo, conveyances, mail, baggage, and people using information-based and physical screening technology and processes. (Protection)
5. Detect WMD, traditional, and emerging threats and hazards of concern using:
    a. A laboratory diagnostic capability and the capacity for food, agricultural (plant / animal),environmental, medical products, and clinical samples
    b. Bio-surveillance systems
    c. CBRNE detection systems
    d. Trained healthcare, emergency medical, veterinary, and environmental laboratory professionals. (Protection)

Forensics and Attribution (Prevention)

Definition: Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source, to include forensic analysis as well as attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts and/or swiftly develop counter-options.

Preliminary Target:

1. Prioritize physical evidence collection and analysis to assist in preventing initial or follow-on terrorist acts.
2. Prioritize CBRNE material (bulk and trace) collection and analysis to assist in preventing initial or follow-on terrorist acts.
3. Prioritize biometric collection and analysis to assist in preventing initial or follow-on terrorist acts.
4. Prioritize digital media, network exploitation, and cyber technical analysis to assist in preventing initial or follow-on terrorist acts.

Access Control and Identity Verification (Protection)

Definition: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

Preliminary Target:

1. Implement and maintain protocols to verify identity and authorize, grant, or deny physical and cyber access to specific locations, information, and networks.

Cybersecurity (Protection)

Definition: Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Preliminary Target:

1. Implement risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.
2. Implement and maintain procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigations, and operations against malicious actors to counter existing and emerging cyber-based threats, consistent with established protocols.

Physical Protective Measures (Protection)

Definition: Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

Preliminary Target:

1. Identify, assess, and mitigate vulnerabilities to incidents through the deployment of physical protective measures.
2. Deploy protective measures commensurate with the risk of an incident and balanced with the complementary aims of enabling commerce and maintaining the civil rights of citizens.

Risk Management for Protection Programs and Activities (Protection)

Definition: Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments.

Preliminary Target:

1. Ensure critical infrastructure sectors and Protection elements have and maintain risk assessment processes to identify and prioritize assets, systems, networks, and functions.
2. Ensure operational activities and critical infrastructure sectors have and maintain appropriate threat, vulnerability, and consequence tools to identify and assess threats, vulnerabilities, and consequences.

Supply Chain Integrity and Security (Protection)

Definition: Strengthen the security and resilience of the supply chain.

Preliminary Target:

1. Secure and make resilient key nodes, methods of transport between nodes, and materials in transit.

Community Resilience (Mitigation)

Definition: Enable the recognition, understanding, communication of, and planning for risk and empower individuals and communities to make informed risk management decisions necessary to adapt to, withstand, and quickly recover from future incidents.

Preliminary Target:

1. Maximize the coverage of the U.S. population that has a localized, risk-informed mitigation plan developed through partnerships across the entire community.
2. Empower individuals and communities to make informed decisions to facilitate actions necessary to adapt to, withstand, and quickly recover from future incidents.

Long-term Vulnerability Reduction (Mitigation)

Definition: Build and sustain resilient systems, communities, and critical infrastructure and key resources lifelines so as to reduce their vulnerability to natural, technological, and human-caused threats and hazards by lessening the likelihood, severity, and duration of the adverse consequences.

Preliminary Target:

1. Achieve a measurable decrease in the long-term vulnerability of the Nation against current baselines amid a growing population base, changing climate conditions, increasing reliance upon information technology, and expanding infrastructure base.

Risk and Disaster Resilience Assessment (Mitigation)

Definition: Assess risk and disaster resilience so that decision makers, responders, and community members can take informed action to reduce their entity's risk and increase their resilience.

Preliminary Target:

1. Ensure that local, state, tribal, territorial, and insular area governments and the top 100 Metropolitan Statistical Areas (MSAs) complete a risk assessment that defines localized vulnerabilities and consequences associated with potential natural, technological, and human-caused threats and hazards to their natural, human, physical, cyber, and socioeconomic interests.

Threats and Hazards Identification (Mitigation)

Definition: Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of a community or entity.

Preliminary Target:

1. Identify the threats and hazards within and across local, state, tribal, territorial, and insular area governments, and the top 100 MSAs, in collaboration with the whole community, against a national standard based on sound science.

Infrastructure Systems (Response, Recovery)

Definition: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Preliminary Target:

1. Decrease and stabilize immediate infrastructure threats to the affected population, to include survivors in the heavily-damaged zone, nearby communities that may be affected by cascading effects, and mass care support facilities and evacuation processing centers with a focus on life-sustainment and congregate care services. (Response)
2. Re-establish critical infrastructure within the affected areas to support ongoing emergency response operations, life sustainment, community functionality, and a transition to recovery. (Response)
3. Provide for the clearance, removal, and disposal of debris. (Response)
4. Formalize partnerships with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to cascading impacts in an efficient manner. (Response)
5. Restore and sustain essential services (public and private) to maintain community functionality. (Recovery)
6. Develop a plan with a specified timeline for redeveloping community infrastructures to contribute to resiliency, accessibility, and sustainability. (Recovery)
7. Provide systems that meet the community needs while minimizing service disruption during restoration within the specified timeline in the recovery plan. (Recovery)

Critical Transportation (Response)

Definition: Provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people and animals, and the delivery of vital response personnel, equipment, and services into the affected areas.

Preliminary Target:

1. Establish physical access through appropriate transportation corridors and deliver required resources to save lives and to meet the needs of disaster survivors.
2. Ensure basic human needs are met, stabilize the incident, transition into recovery for an affected area, and restore basic services and community functionality.
3. Clear debris from any route type, (i.e., road, rail, airfield, port facility, waterway) to facilitate response operations.

Environmental Response / Health and Safety (Response)

Definition: Conduct appropriate measures to ensure the protection of the health and safety of the public and workers, as well as the environment, from all-hazards in support of responder operations and the affected communities.

Preliminary Target:

1. Identify, assess, and mitigate worker health and safety hazards and disseminate health and safety guidance and resources to response and recovery workers.
2. Minimize public exposure to environmental hazards through assessment of the hazards and implementation of public protective actions.
3. Detect, assess, stabilize, and clean up releases of oil and hazardous materials into the environment, including buildings / structures, and properly manage waste.
4. Identify, evaluate, and implement measures to prevent and minimize impacts to the environment, natural and cultural resources, and historic properties from all-hazard emergencies and response operations.

Fatality Management Services (Response)

Definition: Provide fatality management services, including decedent remains recovery and victim identification, working with local, State, tribal, territorial, insular area, and Federal authorities to provide mortuary processes, temporary storage or permanent internment solutions, sharing information with mass care services for the purpose of reunifying family members and caregivers with missing persons / remains, and providing counseling to the bereaved.

Preliminary Target:

1. Establish and maintain operations to recover a significant number of fatalities over a geographically dispersed area.

Fire Management and Suppression (Response)

Definition: Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types, kinds, and complexities while protecting the lives, property, and the environment in the affected area.

Preliminary Target:

1. Provide traditional first response or initial attack firefighting services.
2. Conduct expanded or extended attack firefighting and support operations through coordinated response of fire management and specialized fire suppression resources.
3. Ensure the coordinated deployment of appropriate local, regional, national, and international fire management and fire suppression resources to reinforce firefighting efforts and maintain an appropriate level of protection for subsequent fires.

Logistics and Supply Chain Management (Response)

Definition: Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community staples. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

Preliminary Target:

1. Mobilize and deliver governmental, nongovernmental, and private sector resources to save lives, sustain lives, meet basic human needs, stabilize the incident, and transition to

recovery, to include moving and delivering resources and services to meet the needs of disaster survivors.

2. Enhance public and private resource and services support for an affected area.

Mass Care Services (Response)

Definition: Provide life-sustaining and human services to the affected population, to include hydration, feeding, sheltering, temporary housing, evacuee support, reunification, and distribution of emergency supplies.

Preliminary Target:

1. Move and deliver resources and capabilities to meet the needs of disaster survivors, including individuals with access and functional needs.
2. Establish, staff, and equip emergency shelters and other temporary housing options (including accessible housing) for the affected population.
3. Move from congregate care to non-congregate care alternatives and provide relocation assistance or interim housing solutions for families unable to return to their pre-disaster homes.

Mass Search and Rescue Operations (Response)

Definition: Deliver traditional and atypical search and rescue capabilities, including personnel, services, animals, and assets to survivors in need, with the goal of saving the greatest number of endangered lives in the shortest time possible.

Preliminary Target:

1. Conduct search and rescue operations to locate and rescue persons in distress.
2. Initiate community-based search and rescue support operations across a wide geographically dispersed area.
3. Ensure the synchronized deployment of local, regional, national, and international teams to reinforce ongoing search and rescue efforts and transition to recovery.

On-scene Security, Protection, and Law Enforcement (Response)

Definition: Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.

Preliminary Target:

1. Establish a safe and secure environment in an affected area.
2. Provide and maintain on-scene security and meet the protection needs of the affected population over a geographically dispersed area while eliminating or mitigating the risk of further damage to persons, property, and the environment.

Operational Communications (Response)

Definition: Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impact area and all response forces.

Preliminary Target:

1. Ensure the capacity to communicate with both the emergency response community and the affected populations and establish interoperable voice and data communications between Federal, tribal, State, and local first responders.
2. Re-establish sufficient communications infrastructure within the affected areas to support ongoing life-sustaining activities, provide basic human needs, and transition to recovery.
3. Re-establish critical information networks, including cybersecurity information sharing networks, in order to inform situational awareness, enable incident response, and support the resiliency of key systems.

Public Health, Healthcare, and Emergency Medical Services (Response)

Definition: Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and behavioral health support, and products to all affected populations.

Preliminary Target:

1. Deliver medical countermeasures to exposed populations.
2. Complete triage and initial stabilization of casualties and begin definitive care for those likely to survive their injuries and illness.
3. Return medical surge resources to pre-incident levels, complete health assessments, and identify recovery processes.

Situational Assessment (Response)

Definition: Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

Preliminary Target:

1. Deliver information sufficient to inform decision making regarding immediate lifesaving and life-sustaining activities and engage governmental, private, and civic sector resources within and outside of the affected area to meet basic human needs and stabilize the incident.
2. Deliver enhanced information to reinforce ongoing lifesaving and life-sustaining activities, and engage governmental, private, and civic sector resources within and outside of the affected area to meet basic human needs, stabilize the incident, and transition to recovery.

Economic Recovery (Recovery)

Definition: Return economic and business activities (including food and agriculture) to a healthy state and develop new business and employment opportunities that result in an economically viable community.

Preliminary Target:

1. Conduct a preliminary assessment of economic issues and identify potential inhibitors to fostering stabilization of the affected communities.
2. Ensure the community recovery and mitigation plan(s) incorporates economic revitalization and removes governmental inhibitors to post-disaster economic sustainability, while maintaining the civil rights of citizens.
3. Return affected area's economy within the specified time frame in the recovery plan.

Health and Social Services (Recovery)

Definition: Restore and improve health and social services capabilities and networks to promote the resilience, independence, health (including behavioral health), and well-being of the whole community.

Preliminary Target:

1. Identify affected populations, groups and key partners in short-term, intermediate, and long-term recovery.
2. Complete an assessment of community health and social service needs, and prioritize these needs, including accessibility requirements, based on the whole community's input and participation in the recovery planning process, and develop a comprehensive recovery timeline.
3. Restore health care (including behavioral health), public health, and social services functions.
4. Restore and improve the resilience and sustainability of the health care system and social service capabilities and networks to promote the independence and well-being of community members in accordance with the specified recovery timeline.

Housing (Recovery)

Definition: Implement housing solutions that effectively support the needs of the whole community and contribute to its sustainability and resilience.

Preliminary Target:

1. Assess preliminary housing impacts and needs, identify currently available options for temporary housing, and plan for permanent housing.
2. Ensure community housing recovery plans continue to address interim housing needs, assess options for permanent housing, and define a timeline for achieving a resilient, accessible, and sustainable housing market.

3. Establish a resilient and sustainable housing market that meets the needs of the community, including the need for accessible housing within the specified time frame in the recovery plan.

Natural and Cultural Resources (Recovery)

Definition: Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and executive orders.

Preliminary Target:

1. Implement measures to protect and stabilize records and culturally significant documents, objects, and structures.
2. Mitigate the impacts to and stabilize the natural and cultural resources and conduct a preliminary assessment of the impacts that identifies protections that need to be in place during stabilization through recovery.
3. Complete an assessment of affected natural and cultural resources and develop a timeline for addressing these impacts in a sustainable and resilient manner.
4. Preserve natural and cultural resources as part of an overall community recovery that is achieved through the coordinated efforts of natural and cultural resource experts and the recovery team in accordance with the specified timeline in the recovery plan.

This page is intentionally left blank.

APPENDIX B: AAR / IP SAMPLE

The following AAR / IP Write-Up Sample follows the HSEEP guidance for exercise development and evaluation processes.

Strength: Standard activation procedures for the Yolo County Strategic National Stockpile Plan include alerting each site being used that activation is eminent as soon as possible, so that they have enough time to assign personnel, setup site, and gather supplies. The Health Department followed all standard activation procedures for this drill including California Health Alert Network and Fax communications beginning December 1, 2008.

References:

1. Yolo County Strategic National Stockpile Plan

Analysis: This was helpful for requesting information on procedures that could change from day to day (Example: a California Health Alert Network and Fax message were sent to University of California, Davis Emergency Operations Center staff asking them to provide the procedure for driving access to Freeborn Hall on the day of the drill). Parking permits were then procured by the University and stored (in the front kiosk at the North-Quad entry gate) for county delivery personnel to utilize on the day of the drill. Since the University may have their own staging site on campus for supplies, the delivery gate could change depending on the incident and Point of Delivery site(s) being used. This method of requesting information would be very important during an actual activation.

Area for Improvement: While the activation protocols for this exercise functioned properly in this instance, it is recommended that these procedures be tested with all Push Partner entities, at least annually, so that they are familiar with the procedure.

Analysis: This drill was carefully planned by the University of California, Davis, and the Yolo County Health Department, which enabled all those participating to be knowledgeable of the activation procedures. This method now needs to be tested with other participating jurisdictions so that all are fully aware of the procedure.

Recommendations:

1.2.1. Enroll more site facility administrators into the Health Alert Network and test it regularly.

Strength: This was the first Yolo County Health Department drill where the advertising and messaging about the clinic was completed by an outside entity. The University redistributed information from the Center for Disease Control Web site and local Health Department Public Information Officer in the form of press releases and advertising for the clinic.

References:

1. Center for Disease Control Seasonal Influenza Web site: http://www.cdc.gov/flu
2. UCD Developed Web site: https://extension.ucdavis.edu/subject-areas/health-and-safety

Analysis: Since the University has control over all methods of information distribution on their campus, it was very helpful that they were the entity pushing the message out.

Dissemination methods included writing on chalk boards in class rooms, creating and publicizing social media events, placing ads in the student newspaper, setting up tables with ads prior to the event, posting articles in staff and student newspapers, creating a Web site, posting flyers on campus bulletin boards, posting events on MU electronic "event boards", emailing flyers through student clubs (Honors Challenge, Sororities / Fraternities), distributing flyers through student housing and various other departments, canvassing campus the day before and day of the event to recruit participation, and posting signage at key junctions the day before and day of the event. It is also noteworthy to mention that most of the above-listed actions began on December 1, 2008 (two days before the actual clinic).

Recommendations:

1.3.1. For future exercises, try to get partner agencies to take an active role in information dissemination.

APPENDIX C: ACRONYM LIST

Acronym	Definition
AAR / IP	After-Action Report / Improvement Plan
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
HSEEP	Homeland Security Exercise and Evaluation Program
MSA	Metropolitan Statistical Area
NIMS	National Incident Management System
SitMan	Situation Manual
TTX	Tabletop Exercise
WMD	Weapon of Mass Destruction


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY