

# **NATIONAL PLANNING SCENARIOS:** *Attack Timelines*

Created for Use in National, Federal, State,  
and Local Homeland Security Preparedness Activities

**March 2006**

This page intentionally left blank.

## Contents

Introduction.....		ii
Scenario 1: Nuclear Detonation.....	7(E)	1-1
Scenario 2: Biological Attack.....		2-1
Scenario 3: Biological Disease.....		3-1
Scenario 4: Biological Attack.....		4-1
Scenario 5: Chemical Attack.....		5-1
Scenario 6: Chemical Attack.....	7(E)	6-1
Scenario 7: Chemical Attack.....		7-1
Scenario 8: Chemical Attack.....		8-1
Scenario 9: Natural Disaster.....		9-1
Scenario 10: Natural Disaster.....	7(E)	10-1
Scenario 11: Radiological Attack.....		11-1
Scenario 12: Explosives Attack.....		12-1
Scenario 13: Biological Attack.....	7(E)	13-1
Scenario 14: Biological Attack.....		14-1
Scenario 15: Cyber Attack.....		15-1
Appendix: Scenario Working Group Members.....		A-1

## Introduction

The Federal interagency community has developed 15 all-hazards National Planning Scenarios for use in national, Federal, State, and local homeland security preparedness activities. The scenarios are planning tools and represent the range of potential terrorist attacks and natural disasters and the related impacts that face our Nation. The objective was to develop a *minimum number of credible* scenarios to establish the *range of response requirements* to facilitate preparedness planning.

### **Value of the Scenarios to State and Local Leaders**

The scenarios were designed to help state and local leaders further develop their capacity to prevent acts of terrorism within their communities and to prepare response capabilities to an event should it occur.

These scenarios reflect a rigorous analytical effort by Federal homeland security experts, with reviews by State and local homeland security representatives. However, refinement and revision will be necessary over time to ensure that the scenarios remain accurate, represent the evolving all-hazards threat picture, and embody the capabilities necessary to respond to domestic incidents. In keeping with the congressional mandate that terrorist threats must be “current and real”, the Department of Homeland Security (DHS) is developing a Universal Adversary (UA) database to host and maintain terrorist threat models. At present, the UA database contains six distinct categories of terrorist threats, fifteen specific terrorist group profiles, dossiers on key terrorist actors, in-depth descriptions of tactics employed by each group, and sufficient background information for the generation of exercise related intelligence.

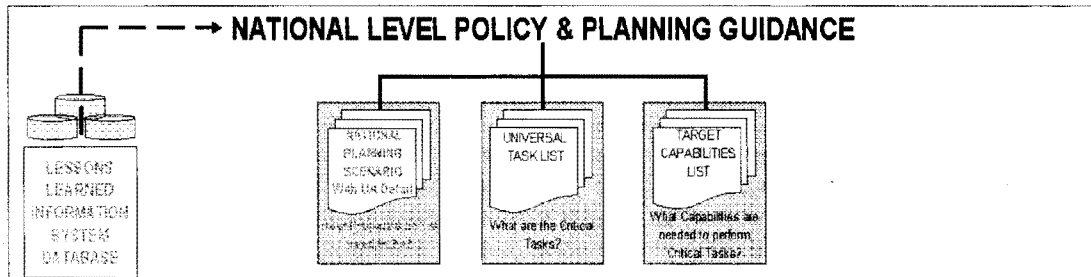
## **The National Planning Scenarios and the Universal Adversary (UA) as Tools in the Capabilities-Based Planning Process**

### **Capabilities-Based Planning**

In seeking to prepare the Nation for terrorist attacks, major disasters, and other emergencies, it is impossible to maintain the highest level of preparedness for all possibilities all of the time. Given limited resources, managing the risk posed by major events is imperative. In an atmosphere of changing and evolving threats, it is vital to build flexible capabilities that will enable the Nation to prevent, respond to, and recover from a range of major events. To address this challenge, DHS employs a capabilities-based planning process that occurs under uncertainty to identify capabilities suitable for a wide range of challenges and circumstances. The process also works within an economic framework that necessitates prioritization and choice. As one of the principal tools in the capabilities-based planning process, the National Planning Scenarios provide a bounded threat universe to address the question: “*How prepared do we need to be?*” Figure 1 depicts the relationship between the scenarios and the other capabilities-based planning tools. As a first step in the capabilities-based planning process, the scenarios, while not exhaustive, provide an illustration of the potential threats for which we must be prepared. The scenarios and the UA database will be used to assess relative risk for the capabilities-



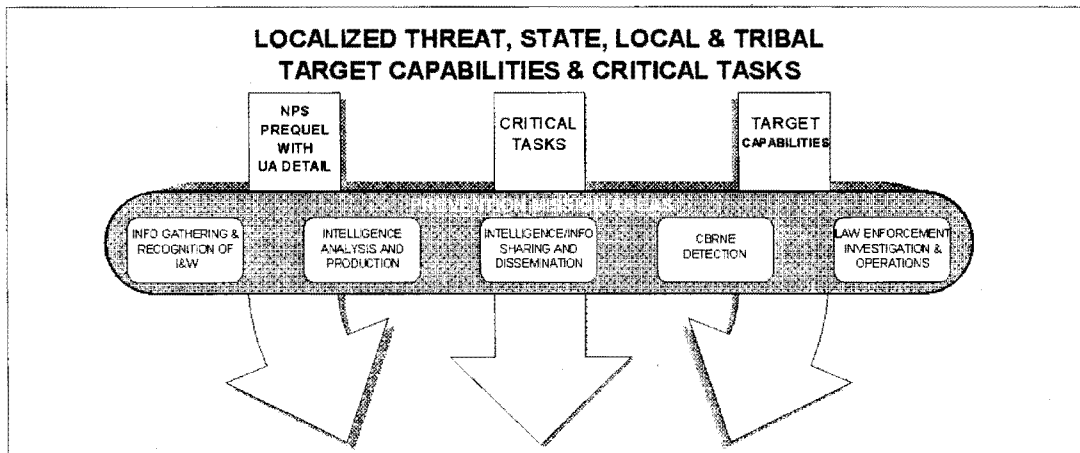
based planning process and provide a framework for appropriately designing and scaling exercises specific to location and population characteristics.



**Figure 1. Tools for the Capabilities-Based Planning Process**

**HSPD-8 Implementation**

The scenarios and the UA database will be used in the implementation of Homeland Security Presidential Directive (HSPD)-8 “National Preparedness,” including the development of the National Preparedness Goal and National Exercise Program. In helping to develop the National Preparedness Goal, the scenarios and the UA database provide the foundation for identifying the capabilities across all mission areas and the target levels of those capabilities needed for effective prevention of, response to, and recovery from major events. Figure 2 illustrates how the scenarios, UA, Target Capabilities List (TCL) and the Universal Task List (UTL) leads planners at all jurisdictional levels to identify common tasks and capabilities for a given mission area, in this instance the Prevention Mission .



**Figure 2. Capabilities-Based Planning and the Prevention Mission**

## **National Planning Scenarios, UA, Red Teams in the National Exercise Program**

In addition to their use as tools in the capabilities-based planning process, the scenarios and the supporting UA also provide the design basis for exercises in the National Exercise Program (NEP). Used as a common foundation for exercise development, the scenarios complemented by current threat information from the UA database ensures exercise participants focus on performing the appropriate critical tasks and will assess capabilities linked to specific homeland security mission areas. The UA detail provided in the following scenarios provides examples of how terrorist groups (or individuals) having the capability, motivation and intent could execute an attack to achieve the outcomes described at the beginning of each scenario. To address exercise design requirements specific to an individual exercise or exercise series, scenario threat models can be modified using current threat information from the UA database. There may be instances when assessing mission critical tasks and capabilities requires employment of analytical or operational Red Teams. The use of Red Teams is prescribed by the *National Strategy for Homeland Security*. Through the application of homeland security intelligence and information, Red Teams view the United States from the perspective of terrorists to discern and predict the methods, means, and targets of potential attackers during government sponsored exercises.<sup>1</sup> Red Teams are comprised of individuals selected for their special subject-matter expertise, perspective (professional, cultural), imagination, and penchant for critical analysis. Red Team members have access to terrorism subject matter experts, intelligence and law enforcement professionals throughout the world, and receive extensive cultural and tactical training in preparation for each exercise event.

### **Employing the Scenarios, UA and Red Team in Prevention Exercises**

Figure 3 provides an example of how the scenarios and the UA are related to the capabilities-based planning process; how the scenarios and UA are used in conjunction with the capabilities-based planning tools to assist state, local and tribal government planning and exercise design and; how the scenarios, the UA and Red Teams are used during the exercise lifecycle of a Prevention Exercise.

---

<sup>1</sup> Office of Homeland Security. *National Strategy for Homeland Security*. July 2002.

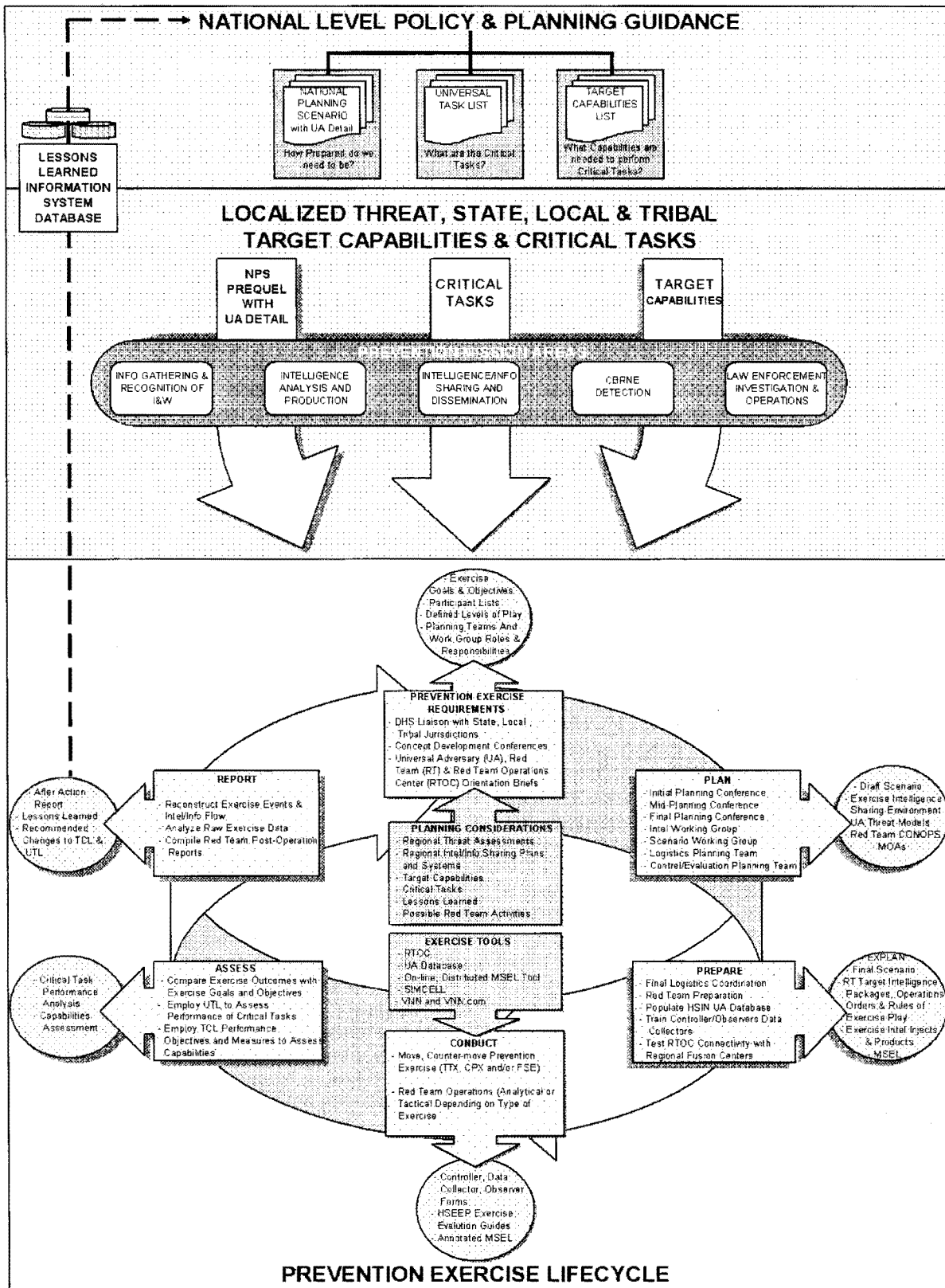


Figure 3. Capabilities-Based Planning and Prevention Exercise Lifecycle

## Considerations

Although not meant to be all-inclusive, the scenarios provide a basic set of common homeland security events and their related impacts that can be employed at the national level or by state, local and tribal jurisdictional authorities. Employing up-to-date information from the UA database, the scenarios have been developed so that they can be adapted to local conditions. Agencies will not be limited to this set of scenarios, and they can exercise scenarios that are not included in the planning set. However, the scenarios provide a mutual starting point for agencies that exercise the basic events included in this set.

### ***Intelligence Disclaimer***

Although the scenarios generally reflect possible terrorist capabilities and known tradecraft, neither the intelligence community nor the law enforcement community is aware of any credible specific intelligence that indicates that such an attack is being planned, or that the agents or devices in question are in possession of any known terrorist group.

### ***Relative Grouping of Scenarios***

Various schemes have been used to rank scenarios based on probability, number of casualties, extent of property damage, economic impact, and social disruption. Because the scenarios in this set were developed to test the full range of response capabilities and resources—and to assist Federal, State, and local governments as well as the private sector in preparing for such events—they have not been ranked.

The groupings of UA elements with specific scenarios are not intended to isolate potential terrorist threats to an individual type or class of terrorist element. Instead, the use of different UA elements is intended to illustrate the many types of capabilities and motivations that might exist.

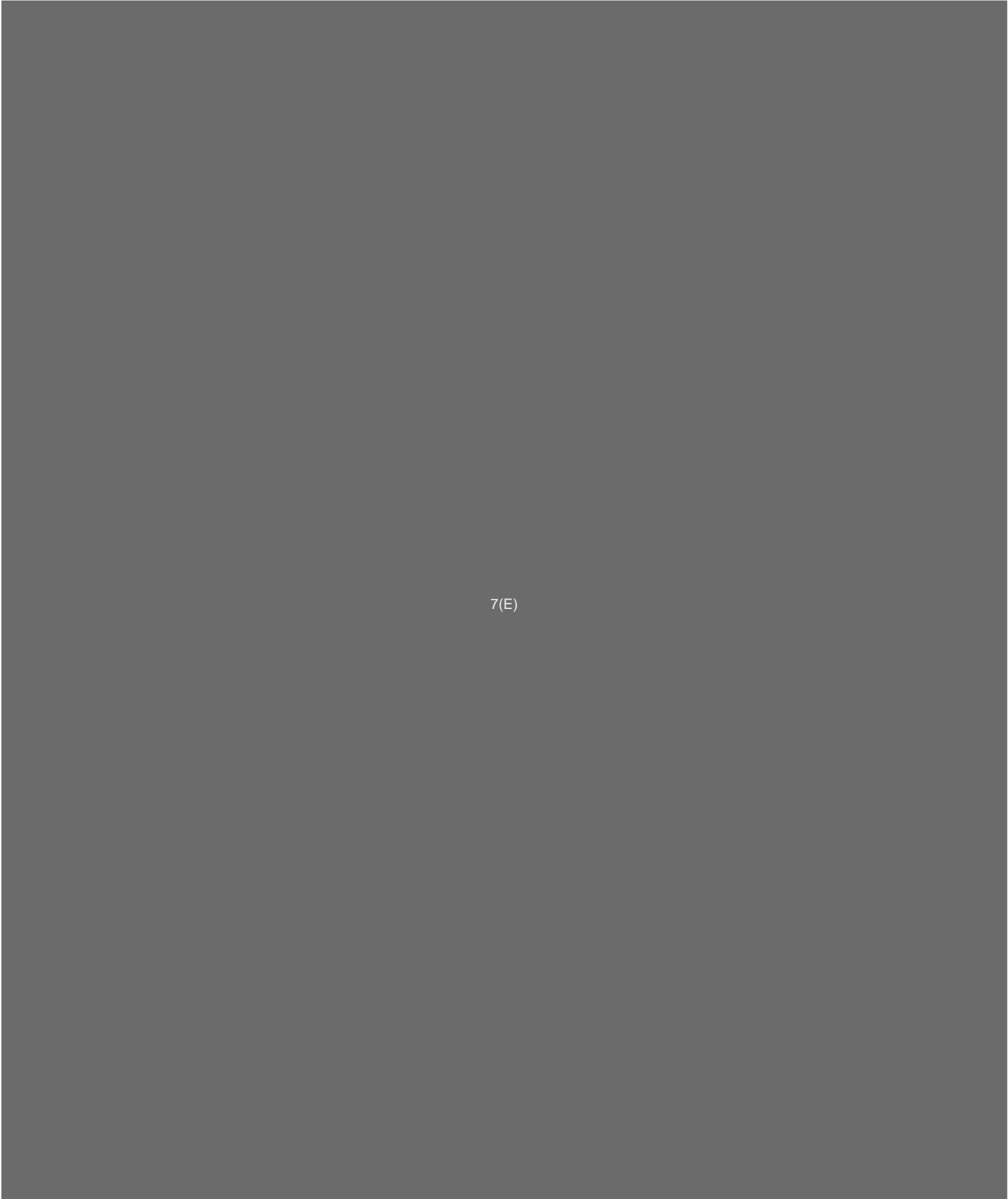
### ***Multiple Events***

In preparedness planning efforts, organizations should always consider the need to respond to multiple incidents of the same type and multiple incidents of different types, at either the same or other geographic locations. These incidents will invariably require the coordination and cooperation of homeland security response organizations across multiple regional, State, and local jurisdictions.

Scenario 1:

# Nuclear Detonation —

7(E)



7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

Scenario 2:

# Biological Attack —

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

ACLURM055329

2-6

**FBI054834**

Scenario 3:

**Biological Disease Outbreak —**

7(E)

7(E)

ACLURM055330

3-1

**FBI054835**

Scenario 4:

**Biological Attack —**

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

ACLURM055339

4-9

**FBI054844**

Scenario 5:

# Chemical Attack —

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

Scenario 6:

# Chemical Attack —

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

Scenario 7:

# Chemical Attack —

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7-11

Scenario 8:

**Chemical Attack —**

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

8-7

Scenario 9:

**Natural Disaster —**

7(E)

7(E)

ACLURM055374

9-1

**FBI054879**

Scenario 10:

**Natural Disaster —**

7(E)

7(E)

10-1

Scenario 11:

# Radiological Attack —

7(E)



7(E)

7(E)

7(E)

ACLURM055378

11-3

**FBI054883**

7(E)

7(E)

7(E)

7(E)

7(E)

11-7

Scenario 12:

# Explosives Attack —

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

12-8

ACLURM055390

**FBI054895**

Scenario 13:

# Biological Attack —

7(E)

7(E)



7(E)

7(E)

13-3

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

13-9

Scenario 14:

**Biological Attack —**

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

14-6

Scenario 15:
<b>Cyber Attack</b>

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)

7(E)



7(E)

7(E)

7(E)

7(E)

7(E)

15-15

# APPENDIX: UA Development Members

The UA and associated scenario prequels were developed by Applied Marine Technologies, Inc. (AMTI), principal contractor to OPIA, DHS. The AMTI team is comprised of personnel from diverse backgrounds, including: special operations planning and execution, intelligence collection and analysis, terrorism and insurgency studies, information technology, Arabic language and culture, screenwriting, research, and journalism.