Homeland Security Exercise and Evaluation Program

Volume V: Prevention Exercises

December 2005

U.S. Department of Homeland Security

Preparedness Directorate

Office of Grants & Training

Table of Contents

Introduction

Following the terrorist attacks in 1995 and 2001 and the establishment of the Department of Homeland Security (DHS) in 2002, homeland security professionals at all levels of government and in all types of communities have been preparing to prevent, protect against, respond to, and recover from a variety of new and existing threats to public safety. The Homeland Security Exercise and Evaluation Program (HSEEP) reference manuals deliver an exercise program that encompasses the lessons learned and best practices of these existing approaches.

The HSEEP reference manuals help homeland security professionals address capabilities built through planning, training, and equipment procurement, and provides them with the tools to plan, conduct, and evaluate exercises to improve overall preparedness. The DHS Preparedness Directorate, Office of Grants and Training (G&T) is responsible for updating and disseminating the HSEEP reference manuals on behalf of DHS.

The HSEEP program and reference manuals integrate language and concepts from the National Response Plan (NRP), National Incident Management System (NIMS), the Universal Task List (UTL), the Target Capabilities List (TCL), existing exercise programs, and representative prevention and response protocols from all levels of government. In the spirit of the NIMS, all efforts should be made to ensure consistent use of the terminology and processes described in HSEEP.

This document is the fifth in a series of HSEEP resources that includes four additional volumes to help Federal, State, local, and tribal jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises. The HSEEP resource documents, available at the DHS Web site (http://www.hseep.dhs.gov) include the following manuals:

> *HSEEP Volume I: HSEEP Overview and Exercise Program Management* provides guidance for building and maintaining an effective exercise program, and summarizes the planning and evaluation process described in further detail in Volumes II through V.
>
> *HSEEP Volume II: Exercise Planning and Conduct* outlines a standardized foundation, design, development, and conduct process adaptable to any type of exercise.
>
> *HSEEP Volume III: Exercise Evaluation and Improvement* offers proven methodology for evaluating and documenting exercises and implementing an improvement plan.
>
> *HSEEP Volume IV: Sample Exercise Documents and Formats* provides sample exercise materials referenced in HSEEP Volumes I, II, III and V.
>
> *HSEEP Volume V: Prevention Exercises* contains guidance consistent with the HSEEP model to assist jurisdictions in designing and evaluating exercises that test prevention capabilities such as intelligence analysis and information sharing.

Recognizing that HSEEP users' range of experience with exercise design and development may vary widely, *Volume V: Prevention Exercises* presents a standardized and straightforward process, adaptable to a wide range of prevention exercise types, scenarios, and resources. This document provides guidance and a uniform approach to prevention exercise foundation, design, development, conduct, and evaluation.

Background

The prevention of terrorist activities and attacks has been given the highest priority in the ongoing effort to increase our Nation's security[1]. Prevention is defined, for purposes of this program as those activities that serve to detect, protect against, and disrupt terrorist threats or actions against the United States and its interests[2]. Activities of terrorists and their supporters have to be detected, identified, and counteracted with prevention activities. These prevention activities span a wide range, from simple background checks to complex, long-term investigations. At the crux of prevention and all the corresponding activities is the ability for agencies and governments to share information. Information sharing is what allows terrorism prevention to function. Effective prevention relies upon the interchange of terrorism information among agencies, and the interchange of terrorism information between agencies and appropriate authorities of States and local governments[3].

Terrorism prevention is no longer the sole purview of the classical anti-terror forces of the federal intelligence community or military. Prevention today involves many players at all levels of government, from the police officer on the street, to the private sector stakeholder, to the intelligence analyst at the Federal, State and local level. All are partners in the national effort to prevent another terrorist attack. In order to make this a concerted, effective effort, all of the players must be able to communicate and share their combined knowledge, and systems used to facilitate the information/intelligence flow must be exercised in order for staff to be knowledgeable, responsive, and comfortable with them.

Improvement in prevention capabilities at the local level is of particular importance as crimes that are isolated to certain localities may illuminate larger patterns. Local experts are essential personnel, as they maintain the ability to fuse knowledge of national threats with local threats, and they control resources needed to act upon operational intelligence. Local-level personnel should work toward contributing their knowledge and understanding of the local threat picture to the larger regional or National effort.

The Prevention Exercise Program (PEP) is dedicated to provide participants at the Federal, State, tribal, and local levels the tools through which to test and improve their ability to prevent terrorism. Exercises are intended to produce comprehensive and valuable analyses of prevention capabilities in order to ultimately enhance the Nation's ability to prevent terrorism by preparing information sharing environment stakeholders at the State and local levels to fuse local and National information and intelligence and produce predictive analysis.

Purpose

The purpose of this manual is to provide homeland security partners at all levels of government and private sector stakeholders the necessary guidance on how to design, develop, conduct, and evaluate prevention exercises. The manual will illustrate the nuances of prevention exercises, explaining their unique characteristics and requirements, and particularly how they differ from response-oriented exercises. In general, it will instruct users on how to use the established HSEEP methodology and tools to create exercises that will evaluate and verifiably enhance their, and the Nation's, ability to fulfill the terrorism prevention mission.

[1] Executive Order 13356: Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans.

[3] Executive Order 13356: Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans.

Information Management Policy

The purpose of the PEP Information Management Policy (IMP) is to establish specific measures that will be implemented to protect sensitive information directly and/or indirectly related to the development, planning and conduct of prevention exercises as well as to define the information management responsibilities of individuals in certain leadership roles. This policy pertains to the creation, compilation, storage, transmission, dissemination and destruction of exercise-related deliverables to include, but not limited to, draft and final versions of emails, meeting minutes, briefings, and exercise documents (i.e., Controller and Evaluator Handbook, Red Team Handbook, Exercise Plan, Exercise Evaluation Guides, After Action Report and Improvement Plan) intended for limited and/or broad distribution internally and/or externally during the course of planning, conducting , and evaluating prevention exercises.

This policy does not supersede that which is set forth in DHS MD 11042.1, SLGCP Policy Memorandum No. 05-06 or other applicable policy directives or memorandum. In accordance with Department of Homeland Security Management Directive 11042.1 and Office of State and Local Government Coordination and Preparedness Policy Memorandum No. 05-06, the intent of the IMP is to limit access to that information which could constitute an indicator of U.S. government intentions, capabilities, operations, activities or otherwise threaten operations security and/or to safeguard information that if compromised could result in a loss of life or compromise an operation[4]. *See Appendix C for further information and guidance for the IMP*.

HSEEP Volume IV

Sample prevention exercise formats and documents referenced throughout this manual are contained in HSEEP Volume IV, available at the DHS Web site (http://www.hseep.dhs.gov). These samples are presented in both example and template formats, and can be used to support the planning process discussed in this manual.

[4] DHS MD 11042.1 Section C, Information Designated as FOUO, §6, Paragraphs C and G

Chapter 1
Prevention Exercise Program

"Intelligence is our first line of defense against terrorism, and we must improve the collection capabilities and analysis of intelligence to protect the security of the United States and its allies".

Senator Saxby Chambliss

Vision

The ability to prevent acts of terror has been identified as a priority in the National Preparedness Goal. The National Preparedness Goal sets targets and objectives for the implementation of Homeland Security Presidential Directive-8 (HSPD-8). To address this mandate to prepare the homeland security community to prevent terrorism, DHS has developed the Prevention Exercise Program (PEP). In support of DHS' other preparedness efforts falling within the prevention mission area, the PEP has been initiated to enhance the preparedness posture of the Nation by addressing the prevention elements of the National Preparedness Goal and the National Incident Management System (NIMS).

PEP is designed to deliver peer-evaluated exercises to homeland security partners using field-validated, collaborative HSEEP tools and methodologies. These exercises are designed based upon participant objectives, to allow participants to learn, demonstrate, and/or validate critical prevention tasks and capabilities. The exercises allow evaluators to produce comprehensive and valuable analyses of prevention capabilities for planning at both the operational and strategic/policy levels. Most importantly, the exercises will substantially and verifiably enhance the Nation's ability to prevent terrorism.

Exercises will be scalable to meet the varying needs and capabilities of the participating jurisdictions, employing many different scenarios and exercise types. Scenarios and injects will be based on a jurisdictional threat analysis, providing realism and further incorporating the specific needs or issues of the jurisdiction into the foundation of the exercise. These exercises will provide near real-time environments to test participant strategies, technologies, plans, policies, and procedures to improve overall national preparedness.

As participants demonstrate improved capabilities and proficiency in increasingly demanding prevention tasks, and the exercises become more complex, the focus of the program will expand to allow evaluators to produce operational-level analyses, addressing the comprehensive system of strategic and tactical issues in the prevention operating environment. To accommodate and continually stress these increasing capabilities, PEP exercises will be augmented over time to provide additional depth and rigor, accommodate more participants, and increase in complexity. The expansion of exercise audiences will enable the exercising of regional agreements and operations, incorporation of private sector partners, and inclusion of appropriate Federal agencies and non-traditional prevention disciplines.

Prevention Core Capabilities

At the root of the Prevention Exercise Program are the prevention core capabilities, which define the specific equipment, personnel, planning, and tasks comprising terrorism prevention that will be exercised. The program will address the express need to exercise certain capabilities and associated critical tasks that are integral to the prevention mission.

Terrorism prevention consists of those activities that serve to detect and disrupt terrorist threats or actions against the U.S. and its interests, and decrease the likelihood that a specific terrorist threat or plan will be culminated or executed. It is these activities that have been identified and consolidated to make up the prevention core capabilities.

The core capabilities required for successful terrorism prevention operations are inherently intertwined. The lines between them are often blurred, with many of the individual capabilities serving functions in more than one mission area. They are not "stove pipe" phases of the prevention operations, but are interdependent and simultaneously occurring elements of the larger antiterrorism mission. The following capabilities have been selected from the Target Capabilities List (TCL) and identified as the prevention core capabilities:

- **Information Gathering and Recognition of Indicators and Warnings (I&W).** Entails the gathering, consolidation, and retention of raw, unexamined data from sources including human-source, observation, and open-source. Recognition of Indicators and Warnings (I&W) is the ability to see in this data the potential indicators and/or warnings of terrorist activities or planning against U.S. citizens, land, infrastructure, and/or allies.
- **Intelligence Analysis and Production.** The merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. This process focuses on the consolidation of analytical products among the intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings.
- **Intelligence/Information Sharing and Dissemination.** The multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the Federal, State, local, and tribal layers of government, the private sector, and citizens. The goals of sharing and dissemination are to facilitate the distribution of relevant, actionable, timely, and preferably declassified or unclassified information and/or intelligence that is updated frequently to consumers that need it. More simply, the goal is to get the right information, to the right people, at the right time.
- **CBRNE Detection.** The capability to defend against weapons of mass destruction (WMD) through deployment of systems to ensure early detection of the import, transport, manufacture, or release of chemical, biological, radiological, nuclear, and explosive materials.
- **Law Enforcement Investigation and Operations.** The broad range of activities undertaken by law enforcement and related entities to detect, examine, probe, investigate, and conduct operations related to potential terrorist activities. Current and emerging investigative techniques are used, with emphasis on training, legal frameworks, recognition of indications and warnings, source development, interdiction, and related issues special to antiterrorism activities.

See the Target Capabilities List for the full details of the Prevention Core Capabilities.

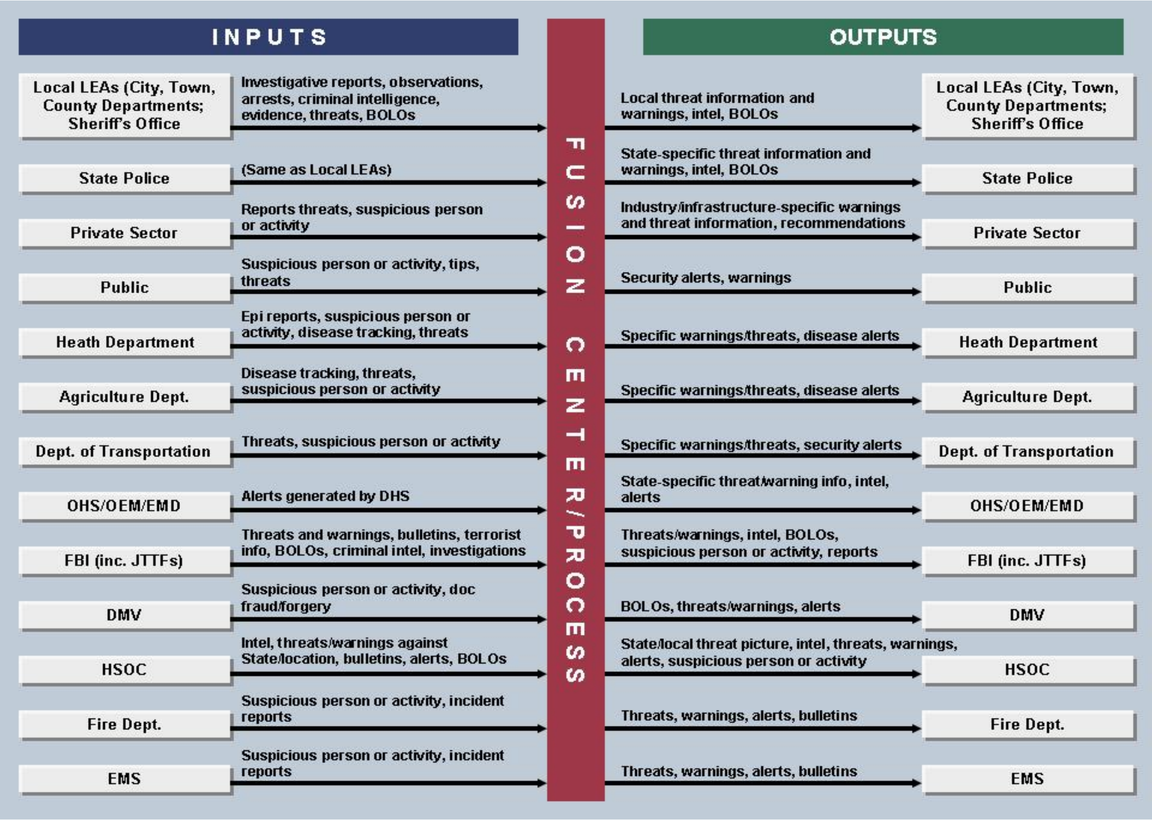
Information Sharing Environment Analysis

The Information Sharing Environment Analysis (ISEA) is a process for jurisdictions to identify and chart their information sharing environment as it pertains to standard operating procedures policies and systems. A comprehensive ISEA can be conducted in coordination between DHS' Office of Grants and Training (G&T) Exercise Division and the Prevention Technical Assistance Program (PTAP). The ISEA should be administered at the appropriate level (e.g., local, State, or regional) prior to an Initial Planning Conference (IPC) of a prevention exercise.

The ISEA is an informative method that seeks to develop the picture of the prevention landscape by answering the following questions:

- What activities encompass all of the exercising jurisdiction's antiterrorism efforts (e.g., outreach programs, internal initiatives, personnel job responsibilities)?
- What agencies, departments, units, and programs support/lead these activities?
- What are the narrowly defined purposes of each of these organizations' participation in these activities?
- What are the administrative, communication, implementation, and interoperable systems that connect these organizations?
- How are these systems physically built, populated with information, accessed by partners, and trained upon? What is the narrowly defined purpose of each system?

Figure 1-1 provides a list of sample information sharing inputs and outputs from various Federal, State and local public and private sector agencies/organizations to be identified during the ISEA.



INPUTS
OUTPUTS
FUSION CENTER/PROCESS
Local LEAs (City, Town, County Departments; Sheriff's Office
Investigative reports, observations, arrests, criminal intelligence, evidence, threats, BOLOs
Local threat information and warnings, intel, BOLOs
Local LEAs (City, Town, County Departments; Sheriff's Office
State Police
(Same as Local LEAs)
State-specific threat information and warnings, intel, BOLOs
State Police
Private Sector
Reports threats, suspicious person or activity
Industry/infrastructure-specific warnings and threat information, recommendations
Private Sector
Public
Suspicious person or activity, tips, threats
Security alerts, warnings
Public
Heath Department
Epi reports, suspicious person or activity, disease tracking, threats
Specific warnings/threats, disease alerts
Heath Department
Agriculture Dept.
Disease tracking, threats, suspicious person or activity
Specific warnings/threats, disease alerts
Agriculture Dept.
Dept. of Transportation
Threats, suspicious person or activity
Specific warnings/threats, security alerts
Dept. of Transportation
OHS/OEM/EMD
Alerts generated by DHS
State-specific threat/warning info, intel, alerts
OHS/OEM/EMD
FBI (inc. JTTFs)
Threats and warnings, bulletins, terrorist info, BOLOs, criminal intel, investigations
Threats/warnings, intel, BOLOs, suspicious person or activity, reports
FBI (inc. JTTFs)
DMV
Suspicious person or activity, doc fraud/forgery
BOLOs, threats/warnings, alerts
DMV
HSOC
Intel, threats/warnings against State/location, bulletins, alerts, BOLOs
State/local threat picture, intel, threats, warnings, alerts, suspicious person or activity
HSOC
Fire Dept.
Suspicious person or activity, incident reports
Threats, warnings, alerts, bulletins
Fire Dept.
EMS
Suspicious person or activity, incident reports
Threats, warnings, alerts, bulletins
EMS

Figure 1-1. Sample Inputs and Outputs of the Local ISE

A typical ISEA product is the ISEA flow chart, depicted in Figure 1-2. This chart illustrates the local information sharing environment, its participants, and its inputs and outputs. The ISEA flow chart should visually illustrate the flow of information or intelligence through formal communication networks both internally (e.g. within a fusion center) and externally (e.g. between fusion center and its local and federal counterparts). Recognizing that some valuable channels may be excluded from this chart, an explanation of some of the informal means of communication or intelligence sharing should also result from the ISEA.

Exercise planners will use the ISEA results to ensure exercise objectives are effectively tailored, capabilities are exercised at an appropriate level, and key systems are realistically tested. The ISEA flow chart will be the foundation for the development of the exercise injects that drive play. Each inject should be crafted to either engage or mimic actual communications mediums, to enhance realism for exercise participants.

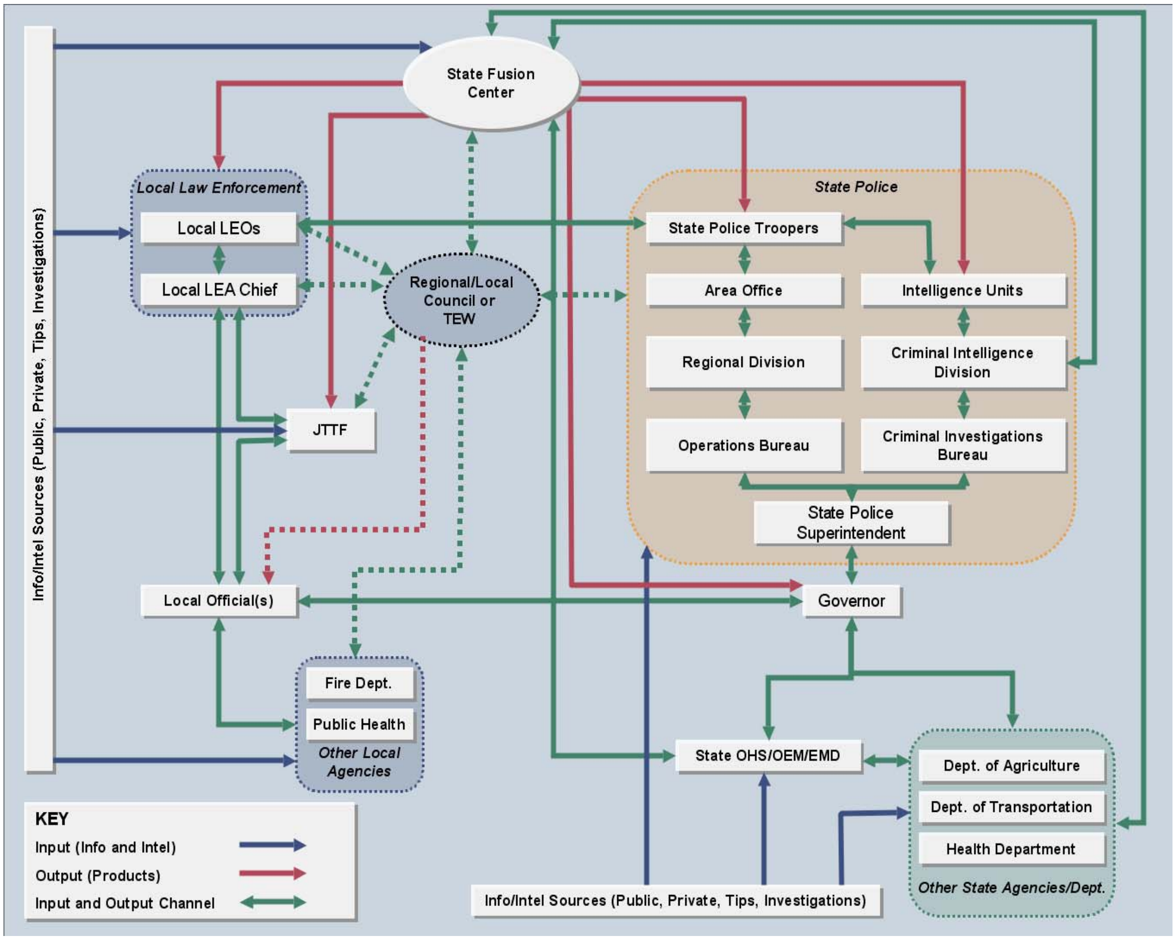


Figure 1-2. Sample ISEA Flow Chart

Implementation Tools

In addition to the implementation tools normally incorporated in response-focused HSEEP exercises, such as the National Planning Scenarios (NPS), capabilities-based planning, the Universal Task List (UTL), Target Capabilities List (TCL), and Exercise Evaluation Guides (EEGs), prevention exercises utilize several unique elements and tools to convey realism and ensure objectives are met. These include the Universal Adversary (UA), Ground Truth, Red Team techniques, Attack Tree analysis, and the Critical Path evaluation. Prevention exercises also make use of standard exercise elements and tools such as the Simulation Cell (Simcell) and Master Scenario Events List (MSEL) that are customized to meet the different needs of prevention exercises. Prevention exercises will use these tools to develop scenarios, conduct play, and collect and analyze data.

Universal Adversary (UA)

The UA is a fictionalized adversary created by compiling known terrorist motivations, doctrine, tactics, techniques, and procedures (TTPs) in live, virtual, and constructive simulations. The UA is based on realistic threats, but it is designed not to compromise actual intelligence. The UA will be utilized for DHS-sponsored exercises, providing participants with a realistic, capabilities-based opponent. Prevention exercises will employ an adaptable, threat-based UA, in some cases represented by physical Red Teams or analytical opponents. The UA reflects real-world uncertainties and unpredictability, and evolving terrorist TTPs. The UA is currently broken into the following five threat groups currently faced by the U.S. within our borders:

- **The Anti-Globalization Movement** is mostly non-violent, but some anarchist groups and more extreme activists have used violence. The national Memorial Institute for the Prevention of Terrorism (MIPT) has catalogued and attributed 70 terrorist events to Anti-Globalization groups from 1998 through 2004, none of which took place in the United States. The Anti-Globalization movement emerged throughout the 1990s and became a serious security threat, as tens of thousands of demonstrators protested Great Eight (G8) Economic Summit in Cologne, the World Trade Organization (WTO) in Seattle, and the International Monetary Fund (IMF) / World Bank in Washington. Police were unprepared for the number of protesters, and unprepared for how well they were organized. While people demonstrated in the streets, companies were suffering thousands of cyberattacks. This mobilization, the sophistication of organization, and highly technical cyber skills overwhelmed law enforcement and security personnel.[1]
- **Domestic Right Wing Extremism**, racist, white-power groups, along with militias, have grown in size and prominence throughout the United States. The number of groups is rising, but the top groups were in decline in 2004. MIPT attributes no terrorist events to Domestic Right Wing groups from 1998 through 2004. The violence perpetrated has been mostly criminal and harassment in nature – vandalism, propaganda fliers, and the occasional physical assault. These attacks are not carried out by groups, but by random individuals inspired by groups' rhetoric. The Southern Poverty Law Center's Intelligence Project counted 762 active hate groups[2] and 152 active Patriot groups[3] in 2004.
- **The Environmental / Animal Rights Movement** has emerged as a serious domestic terrorist threat. Various sources have catalogued and attributed 133 terrorist events to Environmental / Animal Rights groups from 1998 through mid-April 2005. Extremists target government agencies, private companies, academic research institutes, and the

[1] Canadian Security Intelligence Service. "Anti-Globalization – A Spreading Phenomenon." *Perspectives Report #200008.* 22 August 2000. Online at: http://www.csis-scrs.gc.ca/miscdocs/200008_e.html

[2] Southern Poverty Law Center's *Intelligence Project.* Online at: http://www.splcenter.org/intel/map/hate.jsp

[3] Southern Poverty Law Center's *Intelligence Project.* Online at: http://www.splcenter.org/images/dynamic/intel/report/31/patriot_groups_2004.pdf

individuals associated with all three, in direct action to stop animal suffering,[4] or to stop the exploitation and destruction of the natural environment.[5] More recent attacks have targeted "sprawl."[6] Two domestic Environmental / Animal Rights groups are designated as terrorist organizations. The Earth Liberation Front (ELF) and the Animal Liberation Front (ALF) are partner organizations in an increasingly violent Environmental / Animal Rights movement. Neither group has a central leader, central location, or a defined organization. There is no official membership. An individual is considered a member of ELF or ALF based on their belief in the central ideology and their actions.

- **The Global Salafist Jihad (GSJ) Movement** is the predominant threat to the United States. GSJ groups are nontraditional terrorist adversaries driven by a common idea and motivation. It is a movement in which al Qaeda ideologues like bin Laden, al-Zawahiri drive followers to pursue physical jihad. Various sources have catalogued and attributed 225 terrorist events to GSJ groups from 1998 through 2004. Bombings accounted for 141 of these attacks. The second and third most common tactics are Armed Attacks and Kidnappings. Bombings and explosions far outweigh other forms of GSJ groups' attacks, and are happening more frequently and in higher numbers. VBIEDs and IEDs were used in most bomb/explosives attacks.
- **The Lone Actor / Small Group** is a serious threat to United States countermeasures and intelligence capabilities. Acting alone defies infiltration, intervention, or intelligence collection. Various sources have catalogued and attributed 43 terrorist events to Lone Actors or Small Groups from 1998 through 2004. Biological Agents accounted for 14 of the 43 attacks. The second most common attacks are Bombings, accounting for nine attacks, and the third most common attacks are Armed Attacks, with seven.

See the XXX for the full details of the Universal Adversary Program.

Ground Truth

The Ground Truth, in general terms, is comprised of the detailed elements of a prevention exercise scenario that must remain consistent during exercise development and conduct to ensure that realism is maintained and objectives may be met in the unscripted move-countermove exercise environment. The Ground Truth includes the scenario timeline, the local threat environment, and UA threat group, and individual adversary profiles and relationships. Once composed, the Ground Truth is used as the basis for MSEL development and Red Team operations planning, if applicable. *See Chapter 4: Operations-Based Prevention Exercises for further information on the Ground Truth.*

During exercise conduct, a controller – typically the exercise planning team Operations Chief – should act as a Ground Truth Advisor. This person tracks how the adversary (i.e., Red Team) and State and local law enforcement, State and local intelligence analyst, and private industry (i.e., Blue Team) moves and countermoves change the fabric of the exercise environment, potentially creating additional truths. To ensure consistency, each unscripted Master Scenario Events List (MSEL) inject should be vetted by the Ground Truth Advisor.

[4] Animal Liberation Front. *The ALF Primer, Third Edition.* Online at: http://www.animalliberationfront.com/ALFront/ALFPrime.htm

[5] North American Earth Liberation Front Press Office. *Frequently Asked Questions about the Earth Liberation Front (ELF).* 2001. Online at: http://www.animalliberationfront.com/ALFront/ELF/elf_faq.pdf

[6] Dana Hull. "Environmental terrorists a growing movement in West." *The San Jose Mercury News.* 14 March 2005.

In each prevention scenario, a UA will plan and execute an attack during a timeline of activity consistent with that adversary's TTPs and the local threat environment. Generally, the timeline should cover the seven stages of attack planning:

1. **Trigger.** A trigger is an event, situation, or circumstance that motivates a adversary to act. The trigger may be internal to the group, or come from an external source. Potential triggers vary widely depending on the UA and their ideology. For example, Global Salafist Jihadists see the presence or influence of western cultures in traditionally Muslim countries as cause to launch attacks, while single issue extremists focused on environmental rights may view the expansion of logging areas as reason to initiate an attack.
2. **Target parameters.** The target parameters are the variables that govern target selection by generally defining who the adversary will target, what tactics will be used, when the attack will take place, and where the attack will occur. These parameters are usually a reflection of a UA's ideology and are constructed in order to maximize the impact of the particular message an adversary wants to convey.
3. **Target research.** Once target parameters have been established, potential targets must be identified. This is accomplished through a wide range of open source methods and means including data mining via the internet, accessing public records, and conducting physical surveillance. This stage may occur several months or even years before an actual attack.
4. **Specific target selection.** Specific targets are selected based target research and a number of factors, including accessibility, vulnerability, and the physical and psychological effects an attack may have. Usually more than one target is selected to in order to provide the attacker with some flexibility in the event that the environment or situation changes, or if the initial operational plan is compromised.
5. **Development of an operational plan.** In this stage, the UA develops a detailed plan of attack for those targets identified as most viable during the target selection stage. The adversary is likely to begin acquiring the resources and material required to carry out the attack in this stage as well. Physical surveillance of selected targets is likely to continue throughout this phase, even if only periodically to ensure the environment or situation remains unchanged.
6. **Attack execution**. This stage includes the assembly of required weapons or devices; movement of personnel, resources, and materials into the operational area; the conduct "dry runs" or attack rehearsals; conduct of the actual attack; and any escape/evasion as well.
7. **Post-attack analysis.** Following the attack, or attempted attack if the effort was unsuccessful, the adversary will engage in some form of analytical process to identify lessons learned and opportunities for improving tactics, techniques, and procedures for future operations. This stage may also include the communication of the lessons learned to other affiliated groups and exploitation of the attack for propaganda purposes through various media or communication outlets.

Red Teaming

A Red Team is the capability-based analytical or physical manifestation of the UA, which serves as an opposing force for Blue Team personnel. Grounded in the terrorist tactics and protocols of the adversary they are portraying, Red Teams aim to exploit vulnerabilities, exposing areas for improvement, and ultimately hardening the target being exercised. Red Team activities can provide added benefit to a prevention exercise by increasing participants' awareness of the tactics, techniques, and procedures employed by terrorists and criminals unique to the geographical areas in which exercises are conducted.

Historically, the concept of Red Teaming has been used for various purposes, including:

- peer review of a plan or procedure;
- assessing vulnerabilities of structures and/or perimeters;
- assessing vulnerabilities of systems, especially within the information sharing environment;
- testing of security systems by replicating the tactics of adversaries;
- producing a credible and realistic representation of actual events and outcomes; and
- defining a threshold of detection, suspicion, and action.

A Red Team may be defined as:

> *A group of subject-matter experts (SME), with various appropriate disciplinary backgrounds, that provides an independent peer review of plans and processes, acts as a devil's advocate, and knowledgeably role-plays the adversary, using a controlled, realistic interactive process during operations planning, training, and exercising.*[7]

Analytical Red Teaming may occur as part of a discussion-based exercise (e.g., Workshop, TTX) or as a stand-alone activity. This process indoctrinates participants into the mind-set of a specific adversary, modeled upon the results of the threat analysis. Once this perspective has been viably gained, participants use it to build a threat or attack that assaults the plan(s), policy(s), or procedure(s) under examination. Analytical Red Teaming may be conducted by agencies/organizations possessing any level of capability, at a lower cost and shorter time commitment than physical Red Teaming. *See Appendix A for further information on Analytical Red Teaming and its implementation.*

Operations-based exercises can employ physical Red Teams. Physical Red Teams adapt to player decisions and actions according to the prescribed adversary's motivations and tactics, which often provides players with instant feedback. Physical Red Teaming offers the opportunity to engage more participants than Analytical Red Teaming, and to rehearse actual movement of personnel, equipment, and information/intelligence messages. Safety and liability issues must be a primary consideration when considering Physical Red Teaming. *See Appendix B for further information on physical Red Teams and their implementation.*

Attack Trees

The Attack Tree provides the exercise planning team with a visual representation of the anticipated and potential paths the UA can take through the course of the exercise. It maps out a given terrorist attack scenario to show every potential adversary planning step and decision point beginning with the intent to do harm, and ending with – for example, in the case of the improvised explosive device (IED) scenario – a successful detonation. It includes all phases of planning and preparation, and details all options available to the adversary at each decision point,

[7] U.S. Department of Homeland Security. "TOPOFF 3 Frequently Asked Questions." Online at: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0603.xml

including an analysis of the risk, likelihood, and consequences of specific scenario elements.

The Attack Tree serves as the foundation for developing an exercise scenario that accurately portrays real world threats and the objectives needing to be achieved to be successful against that scenario. To this end, it provides detailed information on the specific events, activities, and/or actions that take place leading up to an attack. This information allows exercise planners to develop plausible scenarios and MSEL injects, minimize artificialities, and portray accurate timelines, all of which are essential elements of an effective prevention exercise.

Through the examination of the adversary's options displayed by the Attack Tree, exercise planners can make informed decisions on which of the options they are most likely to face in their jurisdiction, and which ones they are most vulnerable to. Based on these decisions, planners can determine which of their capabilities they want to test in the exercise, including systems, processes, personnel, organizations, etc. Such analysis will ensure that the selected exercise objectives are in line with those options on the Attack Tree that stress the jurisdiction's most vital capabilities. Along the same lines, the Attack Tree provides the basis for evaluation planning and a benchmark against which evaluation tools, such as the Critical Path described below, can be measured. An excerpt from the Prevention IED Attack Tree is depicted in Figure 1-3.

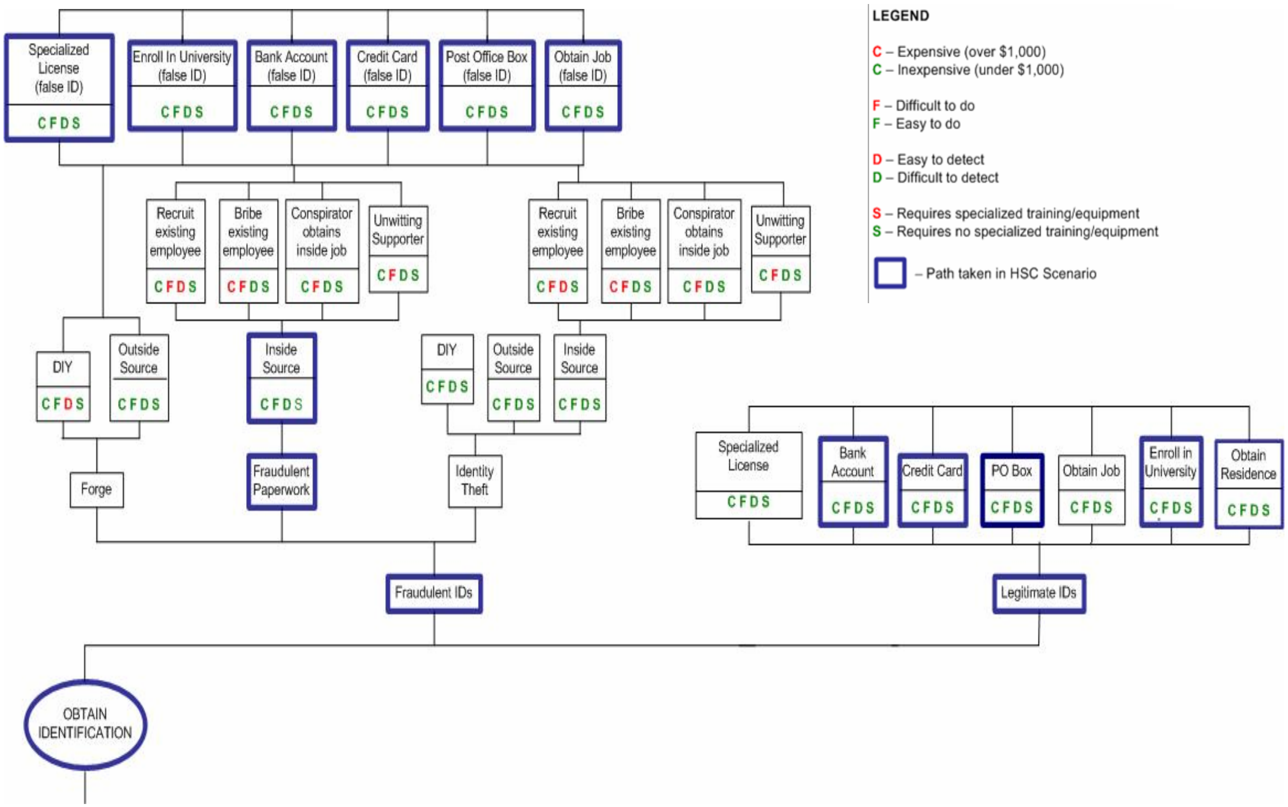


Figure 1-3. Excerpt from Prevention IED Attack Tree

Critical Path

The Critical Path is the map and timeline of Blue Team and Red Team moves and countermoves throughout the course of the exercise, as depicted in the Attack Tree. The Critical Path's use in this capacity begins during exercise design and development, when planners define the "planned" critical path of the exercise scenario based upon the Attack Tree. For the purposes of evaluation, the “planned” critical path serves as the benchmark against which the Blue Team’s capability to exploit prevention opportunities can be measured. As the exercise progresses, Blue Team actions and Red Team reactions can be plotted onto the Attack Tree to create the “exercise” critical path.

At the end of the exercise, the “exercise” critical path can be compared to the “planned” critical path, highlighting any deviations. The final Attack Tree should provide a graphical illustration of those areas in which Blue Team actions did or did not prevent Red Team actions. In some areas, analysis may show that Blue Team actions successfully pushed the Red Team off the planned critical path. These areas could potentially be the source of best practices.

Areas in which Red Team action was not prevented can be analyzed more closely to determine potential deficiencies and plans for improvement. In this way, the Attack Tree is essentially a gap analysis tool. By providing a visual reference illustrating exercise outcomes, the Attack Tree provides a risk-based framework that can be used to help identify those points along the planning trajectory where finite resources can most effectively and efficiently be applied to improve prevention capabilities.

Simulation Cell

A Simcell simulates activity for non-playing entities and coordinates a variety of essential exercise support activities. Since prevention exercises are largely intelligence/information based, Simcells must be able to support an expanded role. Simcells receive and track participant information and inject selected key events during the exercise, as directed in the MSEL. In a prevention exercise, a Simcell may establish the contemporary operating environment; simulate a Federal headquarters or real-world intelligence channel; and/or facilitate Red Team or adversary activities and receive player response. To accurately represent the decisions and actions of simulated entities, prevention exercise Simcells may be modeled after the Homeland Security Operations Center (HSOC), which coordinates the efforts of more than 35 agencies during a real-world incident or threat. *See HSEEP Volume II for further information regarding the use of Simells.*

A Simcell is a location from which phone calls, radio messages, facsimiles, emails, network postings, and other types of messages are delivered from controllers representing actions, activities, and conversations of an individual, agency, or organization that is not participating in the exercise but that would likely be actively involved during a real threat. In the Simcell, controllers track the player and adversary moves initiated by each inject. This is most effectively done by utilizing the tracking component of the MSEL Tool. Because MSELs are organized by inject number, tracking exercise play as it is relative to the MSEL ensures that data can be queried in any necessary way. Such queries provide information to exercise controllers that enables them to alter the scenario as needed in reaction to a change in the threat environment, review what information Red Team or Blue Team has uncovered, find trends that should be addressed in the AAR, or determine any number of other factors.

Master Scenario Events List (MSEL)

The MSEL complements the Attack Tree, which graphically maps out multiple potential courses of action for the UA. Thus, the MSEL affords flexibility for move-countermove interaction between the Red and Blue Teams and is heavily populated with contingent events at the outset of the exercise to account for these potential variables and courses of action. At the end of the exercise, the injects that were entered into play and the events that occurred in response constitute the substance of the exercise Critical Path. *See Chapter 2: Prevention Exercise Planning Process* *and Chapter 4: Operations-Based Prevention Exercises for more information on the development and management of the MSEL.*

Chapter 2

Prevention Exercise Planning Process

The following chapter outlines the necessary steps and milestones associated with the successful foundation, design, development, conduct, and evaluation of a prevention exercise. More detailed descriptions of fundamental exercise planning concepts and materials addressed in this section are available in *HSEEP Volume II: Exercise Planning Process*.

Exercise Planning Team

The exercise planning team is responsible for designing, developing, conducting, and evaluating all aspects of an exercise. Members of the exercise planning team:

- determine exercise objectives;
- tailor the scenario and Universal Adversary (UA) profile to meet the exercising jurisdiction/organization's needs;
- develop documentation used in evaluating, controlling, and simulating;
- develop and distribute pre-exercise materials;
- conduct exercise planning conferences, briefings, and training sessions; and
- serve in controller, evaluator, and Red Team controller/operative positions.

The planning team is managed by a Lead Exercise Planner. The planning team should be of manageable size and should include a representative from each of the major participating agencies, jurisdictions, and organizations.

Selection of planning team members for prevention exercises should be carefully considered. Planning team members are often chosen from leadership roles in the exercising organizations. Membership in the exercise planning team will preclude these individuals from serving as exercise participants. This can be problematic however, because prevention exercises employ scenarios that prompt management-level officials to make command decisions that affect the remainder of exercise play. Thus, if management-level individuals are employed as planning team members it is essential that a designee exercise participant understand that he/she will perform this decision-making role in the context of the exercise scenario. *See HSEEP Volume II: Exercise Planning Process for further information on identification of the Exercise Planning Team.*

Organizational Structure

The exercise planning team must be provided with clearly stated roles and responsibilities, along with assigned tasks and completion timelines. The Lead Exercise Planner may create an Exercise Project Management Timeline and an Exercise Project Management Assignment List to ensure that tasks are not overlooked, forgotten, or identified only at the last minute. *See HSEEP Volume IV for Prevention Exercise Project Management Timeline and Exercise Project Management Assignment List samples.*

Exercise planning teams are most efficient when certain core groups with specific assigned responsibilities are formed. As in all HSEEP exercises, the recommended core groups are based upon the Incident Command Structure (ICS) structure. Figure 2-1 provides a foundational structure of the Prevention Exercise Planning Team. The planning team member titles are listed in bold. They correspond to recommended roles for planning team members to play during exercise conduct, listed in italics.

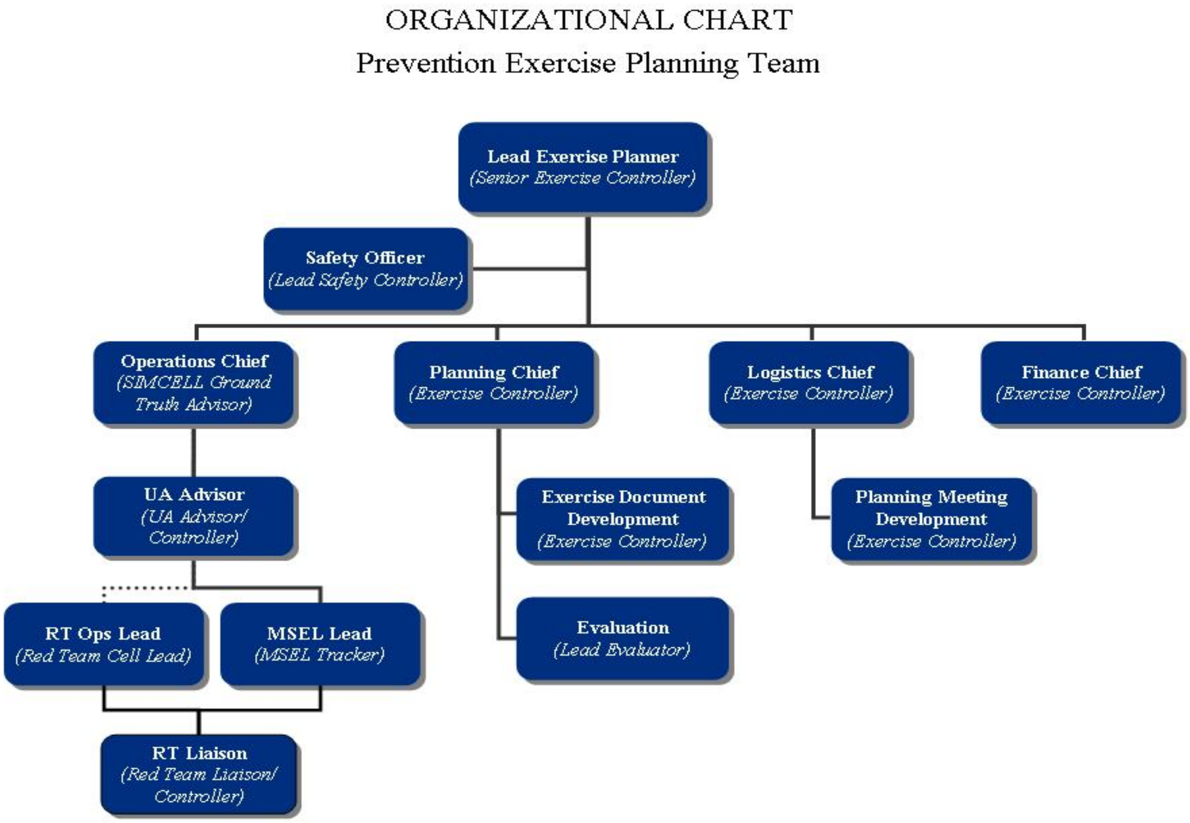


Figure 2-1. Prevention Exercise Planning Team Organizational Chart

The core groups described below provide the basis for potential expansion of the planning team as needed in order to match the scope of the exercise:

- **Command Group:** This group, also referred to as the core planning group, is responsible for coordination of all exercise planning activities. The command group consists of the following roles and responsibilities:
    - ***Lead Exercise Planner.*** The Lead Exercise Planner develops the Exercise Project Management Timeline and the Exercise Project Management Assignment List, assigns exercise tasks and responsibilities, provides overall guidance, establishes timelines, and monitors the development process.
    - ***Operations Chief.*** The Operations Chief oversees development of the exercise scenario and its delivery methods (e.g. Red Team operations and MSEL injects). Because of this s/he should possess subject matter expertise regarding the local threat environment. The Operations Chief also produces and monitors simulations during the exercise. *Note: The Operations Chief acts as a firewall between the Red Team and the exercise planning team in order to maintain the realistic separation between the exercise participants (Blue Team) and their adversaries. This separation is*

intended to ensure that the Red Team accurately tests vulnerabilities by realistically developing their attack plans based on open-source information only.

  - ***Planning Chief.*** The Planning Chief liaises with the other groups to ensure the necessary background information is collected for exercise document development, exercise planning conference conduct, and evaluation planning.
  - ***Logistics Chief.*** The Logistics Chief is ultimately responsible for all logistical issues related to the planning, conduct, and follow-up activities of the exercise.
  - ***Finance Chief.*** The Finance Chief provides grant management and administrative support throughout exercise development.
  - ***Safety Officer.*** The Safety Officer is responsible for developing and enforcing exercise safety policies and ensuring the overall safety and security of the exercise. While planning exercises employing physical Red Teams, the Safety Officer should regularly coordinate with the Red Team Operations Lead and Red Team Liaison (defined below) in order to address the Red Team's specific safety and security needs.

- **Operations Group:** This group provides most of the technical or functional expertise for the participating agencies or jurisdictions. The Operations Group ensures the MSEL and Red Team activities are coordinated with each other and consistent with the exercising jurisdiction's information sharing environment.
  - ***Operations Chief.*** See description above.
  - ***Red Team Operations Lead.*** The Red Team Operations Lead is responsible for defining Red Team concepts, scope, and logistical and safety requirements, based upon limited input from the exercise planning team. The Red Team Operations Lead selects and trains Red Team members, and oversees Red Team operation planning and documentation, but is not privy to information that directs Blue Team exercise development and conduct. *See Appendix A for information on planning and conducting Red Team activities.*
  - ***Red Team Liaison.*** The Red Team Liaison functions as the Red Team point of contact with the rest of the exercise planning team. Because this position is part of the exercise planning team, the liaison must be cognizant not to inadvertently share exercise sensitive information with the Red Team or the Red Team Operations Lead. From the SIMCELL, the Red Team Liaison supports the logistics- and safety-related elements of Red Team activities during exercise play.
  - ***MSEL Lead.*** The MSEL Lead is charged with overseeing the development of the MSEL. They must incorporate the key events of the exercise scenario and include the expected actions of multiple agencies and organizations, as well as those of the Red Team. *See Chapter 4 for information on MSEL development.*
  - ***UA Advisor.*** If a hypothetical adversary is employed, a UA Advisor must be selected to compile the appropriate information for realistic portrayal and consistent use of the adversary over the course of the exercise. The UA Advisor is responsible for providing the MSEL Lead with the overarching scenario and timeline. Once approved by the Operations Chief, this tool becomes a documentation of the ground truth, with which other exercise documentation and activities must remain consistent. The UA Advisor also informs the Red Team Operations Lead of the adversarial roles and characteristics the Red Team will portray.

- **Planning Group:** The planning group is responsible for the exercise design, development, evaluation, and improvement process. Generally, this includes the collection and review of policies, plans, and procedures, development of exercise documentation, training of evaluators, and drafting of the after action report (AAR).
    - ***Planning Chief.*** See description above.
    - ***Exercise Document Development Lead.*** The Exercise Document Development Lead controls the development processes of all exercise documentation and materials, from the initial drafting phases through printing and distribution. *See Chapters 3 and 4 for descriptions of exercise documentation and materials.*
    - ***Lead Evaluator.*** The Lead Evaluator selects and customizes EEGs, assigns evaluators to the appropriate location, collects and analyzes evaluator-collected data, and drafts the AAR. The Lead Evaluator is responsible for collecting and analyzing the information gathered by the field evaluators for the purpose of determining whether the objectives of the exercise are being met, and if so, to what extent. Ultimately, the Lead Evaluator will have to assess and assign a rating on the overall performance of the exercise objectives.
- **Logistics Group:** The logistics group provides the supplies, materials, facilities, and services that enable the exercise and planning conferences to function smoothly without outside interference or disruption. Responsibilities of the logistics group include, but are not limited to transportation, security, signage, food and drinks, real-life medical capability, communications, purchasing, general supplies, media and Very Important Person (VIP)/observer processing, and recruitment/management of exercise personnel.
    - ***Logistics Chief.*** See description above.
    - ***Planning Meeting Development Lead.*** The Planning Meeting Development Lead is responsible for the planning and scheduling for all exercise planning meetings or conferences. They will reserve meeting locations, arrange lodging, and provide necessary meeting items (e.g., projectors, notebooks, pens).
- **Administration/Finance Group:** The administration/finance group provides grant management and administrative support throughout exercise development. This group is also responsible for the participant registration process at both planning conferences and the exercise, and coordinates schedules in consideration of the planning team, Lead Exercise Planner, participating agencies, and the host community(s).

During the planning process, the planning team may expand to include individuals who can help vet the information included in the exercise scenario and injects, the channels for information sharing, and the roles and responsibilities of the players. These individuals include, but are not limited to SMEs from participating and simulated functional areas and personnel with access to certain databases who can ensure all individual and organizational names used for the UA and Red Teams are fictional.

Like many other large, complex, or multi-jurisdictional exercises, prevention exercises may start with a planning team that fills most, if not all, of the sample organizational structure depicted in Figure 2-1. In these cases, section chiefs and others in leadership roles must be prepared to delegate responsibility. The planning team roles delineated in Figure 2-1 have been paired with suggested exercise conduct roles – displayed in italics – for each team member.

Planning Conferences

This section describes the types of planning conferences commonly employed in the design and development of prevention exercises. Four planning conferences, in combination with regular exercise planning team communication, are typically sufficient during exercise design and development. Descriptions of six different planning conferences are listed chronologically in this section. The Lead Exercise Planner and the exercise planning team should decide on the number of meetings needed to successfully conduct a given exercise, considering the exercise scope, its objectives, and the capabilities of the exercising jurisdiction.

Listed below are basic descriptions and the primary objectives for each type of planning conference along with suggested tools which may assist in their conduct. Providing advance information in the form of a read-ahead packet to the planning team members significantly enhances the efficiency of a planning conference; however, the content should follow the information management policy detailed in Chapter 1. *See Appendix C for details regarding the Information Management Policy.*

Concept and Objectives Meeting

A Concept and Objectives (C&O) Meeting is held to identify the type, scope, objectives, and purpose of the exercise and is the formal beginning of the planning process. The C&O Meeting is typically attended by representatives of the sponsoring agency/organization, the Lead Exercise Planner, and senior officials. The C&O Meeting should help planners identify an overall exercise goal, develop rough drafts of exercise objectives, and identify exercise planning team members. The C&O Meeting should also provide an opportunity to answer general questions senior officials may have about prevention exercises.

Depending on the scope of the exercise, the C&O Meeting can range from 2 to 4 hours. Location is determined by the Lead Exercise Planner in consideration of the senior officials in attendance.

Possible topics or issues for a C&O Meeting include:

- Exercise purpose
- Capabilities to exercise
- Proposed scenario, goals, and objectives
- The exercise planning process (e.g., planning conferences, conduct, evaluation)
- Exercise location, date, and duration
- Principles of a prevention exercise (e.g., assumptions and artificialities)
- Control and evaluation
- Security organization and structure
- Local issues, concerns, and sensitivities
- Logistics
- Support from executive leadership

Depending on attendees' familiarity with PEP concepts and local antiterrorism efforts, provision of some of the following read-ahead materials may enhance discussion during a C&O Meeting:

- The multimedia presentation intended for use during the C&O Meeting

- The prevention mission area capabilities from the TCL
- The proposed UA profile from *HSEEP Volume IV*, or a description/open source intelligence on a local adversary which the exercise could model
- A memo on the ISEA process, detailing what information must be gathered and which agencies/departments will be solicited for it. This memo may include a request for consent to be given in order to conduct the ISEA
- A proposed exercise planning team organizational chart, detailing which agencies/departments may provide staff to fill the delineated roles
- Appendices A and B of this manual, *Analytical/Physical Red Teaming*, and/or potential Red Team operations

The following outcomes are expected from the C&O Meeting:

- Sanctioning of/concurrence upon exercise type, scope, scenario, and goals
- Reaching consensus upon the target exercise timeframe and the date and time of the Initial Planning Conference (IPC)
- Identification of exercise participants (individuals and organizations)

Minutes recording the discussions and conclusions of the C&O Meeting should be prepared and disseminated among the attendees and other potential planning team members within 4 working days of the meeting's close. In the period between the C&O Meeting and the IPC, the Lead Exercise Planner will ensure the exercise planning team has sufficient representation from participating agencies/organizations and develop read-ahead materials for the IPC.

Initial Planning Conference

The purpose of the IPC is to gather input from the exercise planning team on the scope, design requirements and conditions (based upon the ISEA), objectives, level of participation, and scenario variables (e.g., adversary, timeline, targets). The IPC is also used to obtain the planning team's input on exercise location, schedule, duration, and other details required to develop exercise documentation.

The best way to determine the design requirements and conditions is by conducting an ISEA. If this process has not already been completed during development of the Prevention Exercise Program, it should begin no later than the IPC. The ISEA flow chart provides the essential information needed by the exercise planning team to accurately depict the local information sharing environment, its participants, and its inputs and outputs. Exercise planners will also use ISEA results to ensure objectives are effectively tailored, capabilities are exercised at an appropriate level, and key systems are realistically tested. *See Chapter 1 for a description of the Information Sharing Environment Analysis (ISEA) and the ISEA flow chart.*

During the IPC, planning team members are assigned responsibility for tasks associated with designing and developing exercise documents and logistics. In particular, the planning team may designate an individual or group to construct the MSEL. When Red Teams will be employed, the Red Team liaison should be identified at the IPC, and Red Team operators should attend no further planning conferences.

Depending on the scope of the exercise, the duration of the IPC can range from 3 to 6 hours. Possible topics or issues for an IPC include:

- Understanding the need and purpose for exercise, and the overarching threat(s) upon which it will be developed
- Ensuring objectives are clearly defined and measurable
- Identifying scenario variables (e.g., adversary profile, timeline, targets, conditions)
- Identifying local issues, concerns, or sensitivities
- Ensuring that exercise planners consider themselves "trusted agents" and understand that, in most cases, they will participate as facilitators, controllers, or evaluators and not as participants
- Identifying participants, SMEs, and additional needs for facilitators, controllers, or evaluators
- Deciding whether to record exercise proceedings (audio or video)
- Determining the optimum duration of the exercise
- Understanding the exercise will be conducted in a no-fault environment intended to validate plans and procedures (through discussion and/or actual demonstration) and identify problems and potential solutions
- Customizing evaluation tool(s) so that they will be able to accurately measure whether proposed exercise objectives were achieved and allow participants to provide feedback
- Developing a planning schedule, determining the best method for communication among the team, and assigning responsibility for exercise documents
- Reaching a consensus regarding the date, time, and location of the next conference and identifying critical tasks for completion by the next conference
- Identifying and assigning responsibility for logistical issues
- Identify document classification procedures (if not discussed in the C&O)

IPC minutes should be prepared and disseminated among planning team members within 4 working days of conference conclusion. Direct and continual contact should occur among all members of the exercise planning team regarding outstanding information and the logistics for conducting additional planning conferences and the exercise itself.

In the period between the IPC and the next conference, exercise planning team members will prepare their assigned draft exercise documents and presentations, described in *Chapter 4: Operation-Based Prevention Exercises*. *See HSEEP Volume II for a detailed description of an IPC.*

Mid-Term Planning Conference

Mid-Term Planning Conferences (MPCs) provide additional opportunities to settle logistical and organizational issues that arise during planning. The MPC is a working session for discussion of exercise organization and staffing concepts, scenario and timeline development, scheduling, logistics, and administrative requirements. It is also a session to review draft exercise documentation.

The MPC is generally a full-day conference, with sufficient time scheduled for conducting a walkthrough of the fusion center and gathering supporting document templates for injects, maps, logos, and other visual aids. The MPC should be held at, or near, the fusion center to facilitate this walkthrough.

Possible topics or issues for an MPC include:

- Commenting on draft exercise documentation
- Any issues regarding the exercise location (e.g., access, potential for player to overhear exercise sensitive information)
- Agreement upon final logistical items
- Assignment of additional responsibilities
- Overview and construction of the scenario timeline and Red Team operations, and agreement upon key scenario injects, in preparation for the MSEL Conference
- Finalization of date, time, and location of the Red Team Conference, MSEL Conference and/or Final Planning Conference (FPC)

MPC minutes should be prepared and distributed to the planning team within 4 working days of conference conclusion. The time between the MPC and the next planning meeting should be used to finalize the remaining exercise documentation and address identified logistical issues. *See HSEEP Volume II for a detailed description of an MPC.*

Red Team Planning Conference

When Red Team activities will be conducted during a prevention exercise, it is essential to confirm the safety redundancies, rules of exercise play (ROEP), Red Team operation plans, and conduct of the operations over the exercise timeline. The exercise planning team should have the opportunity to approve these items either during the MPC or at a subsequent Red Team Planning Conference.

The Red Team Planning Conference is led by the Operations Chief and/or the Red Team Liaison. The Red Team Operations Lead may present specifics on the planned Red Team operations, but s/he should not be privy to any additional exercise-sensitive information discussed or decisions made. If given the level of access afforded to the rest of the exercise planning team, the Red Team would become aware of law enforcement prevention plans, procedures, and capabilities which would give them unrealistic insight and advantage.

A Red Team Planning Conference usually lasts 2 to 4 hours, depending on the number of operations proposed. *See Appendix B of this manual, Physical Red Teaming for more information on safety redundancies, ROEP, and Red Team operation plans.*

Red Team Planning Conference minutes should be prepared and distributed to the planning team within 4 working days of conference conclusion. Final drafts of the ROEP and Red Team operation plans should be prepared and distributed to the planning team prior to the next planning conference.

Master Scenario Events List Conference

A Master Scenario Events List (MSEL) Conference is extremely important in the planning process of a prevention exercise. During a MSEL Conference key members of the Operations Group should meet with SMEs from the exercising fusion center to review the scenario timeline. The entire exercise planning team is not needed for a MSEL Conference; in fact, attendance by too many individuals has been shown to hinder consensus and progress. One individual should be assigned the task of incorporating the outcomes of the Conference into the MSEL. The final draft of the MSEL should be presented at the FPC for the exercise planning team to approve.

As discussed in Chapter 4, the MSEL is a chronological list that controls how the exercise scenario unfolds by providing controllers and evaluators with event synopses, expected participant responses, objectives to be addressed, and personnel responsible for implementing the events. It includes scenario events that will prompt players to implement the plans, policies, and procedures that planners want the exercise to test. It also records the methods that will be used to inject each particular event (e.g., phone call, fax, network transmission, e-mail).

The length of a MSEL Conference varies according to the scope of the exercise and variability of the injects. Attendees of the MSEL Conference should be provided with the Ground Truth document, draft report of MSEL injects that have been developed, and detailed of approved Red Team operations plan. *See Appendix B for information on developing Red Team operations plans.*

The state of a MSEL will vary following a MSEL Conference. At a minimum, all key events and the time of their delivery should be identified and confirmed, and responsibility for constructing/editing the remaining MSEL events should be assigned. It is essential that the final MSEL be reviewed with quality assurance procedures in mind. *See Chapter 4 of this manual for more information on MSELs.*

Final Planning Conference

The FPC provides the final forum for reviewing exercise conduct procedures. The planning team will receive final drafts of all exercise materials prior to the FPC. No major changes to the design or scope of the exercise or its supporting documentation should take place at the FPC. The FPC ensures that all logistical requirements have been arranged for, all outstanding issues have been identified and resolved, and all exercise products are ready for printing.

The FPC should be a full day conference for prevention exercises. It should be located in close proximity to the exercising fusion center in case a final walkthrough becomes necessary.

The following items should be addressed at the FPC:

- Resolve any open issues related to exercise planning and identify last-minute concerns that may arise
- Review all exercise logistical and administrative tasks
- Conduct a comprehensive final review of all exercise documents and approve them for printing and distribution
- Ensure a clear understanding of exercise conduct procedures and provide approval to continue planning Red Team operations

FPC minutes should be prepared and disseminated among exercise planning team members within 4 working days of the conference’s conclusion. Direct and frequent contact should be maintained among exercise planning team members following the FPC and leading up to the exercise to ensure that all final tasks are satisfactorily completed. Prior to the exercise, information and documentation should be disseminated to players, facilitators, controllers, evaluators, and Red Team operators, as appropriate. *See HSEEP Volume II for a detailed description of an FPC.*

Chapter 3

Discussion-based Prevention Exercises

To Be Developed at a Future Date

Chapter 4

Operations-Based Prevention Exercises

Similar to response-focused operations-based exercises, the planning phases of an operations-based prevention exercise include foundation, design and development, conduct, evaluation, and improvement. The distinctions between response-focused exercise planning and prevention exercise planning includes the implementation of prevention tools (e.g., Universal Adversary (UA), Ground Truth, Red Teaming, Attack Tree, and Critical Path), and the potential extension of the duration of exercise play.

The characteristics and tools unique to prevention exercises were developed to compliment the Office of Grants and Training (G&T) Homeland Security Exercise and Evaluation Program (HSEEP). For that reason, prevention exercise planners should employ the HSEEP methodology for planning, conduct, and evaluation. This manual provides guidance on the unique characteristics and requirements of prevention exercises.

Foundation

A solid foundation for exercise design is built upon the identification of the appropriate planning team, development and adherence to a schedule of planning conferences, establishment of milestones, and employment of project management tools. The following sections identify tools for effective project management and hyperlinks to various recommended charts, timelines, collaboration aides, and checklists. *See Chapter 2 Prevention Exercise Planning Process for more detail information on exercise foundation.*

Exercise Planning Team

The exercise planning team for a prevention exercise should include representatives from each participating agency/organization or functional area as well as from all necessary logistical support areas. Due to the nature of prevention exercises, the majority of the exercise planning team will consist of law enforcement personnel; however, as dictated by exercise scope and objectives, public and private sector agencies and organizations (e.g., emergency management, fire, media, private security organizations, and private industry) should participate.

Initial discussions to identify the exercise planning team should begin at the Concepts and Objectives Meeting and the exercise planning team should be confirmed and in place prior to the Initial planning Conference. *See Chapter 2 Prevention Exercise Planning Process for a sample prevention exercise planning team organizational chart.*

Planning Conferences

Operations-based prevention exercises are typically planned using a minimum of four conferences: an Initial Planning Conference (IPC), a Mid-Term Planning Conference (MPC), and a Final Planning Conference (FPC), and any combination of a Concept and Objectives (C&O) Meeting, Red Team Conference, and/or Master Scenario Events List (MSEL) Conference, as necessary. Because a large amount of unique information is needed to organize a prevention exercise, as many as six conferences may be scheduled. *See Chapter 2 Prevention Exercise Planning Process for a comprehensive description of prevention planning conferences.*

Project Management

Prevention exercises require a much more detailed and organized planning process than most response-focused operations-based exercises, due to the direct correlation between the Ground Truth document, Attack Tree, MSEL and Red Team operations. An Exercise Project Management Timeline that identifies key planning meeting dates and milestones, and critical tasks should be established by the exercise planning team no later than the conclusion of the IPC. Responsibility for these tasks may be assigned and tracked on an Exercise Project Management Assignment List. Once established, planners must adhere to the scheduled Timeline and Assignment List. Any changes must be justified to the Lead Exercise Planner, and the entire team should be notified to avoid any confusion. *See HSEEP Volume IV for sample Exercise Project Management Timelines and Exercise Project Management Assignment Lists for prevention operations-based exercises.*

Design and Development

The design and development process should build upon the established foundation for the exercise with the identification of exercise design objectives, development of the Ground Truth, creation of exercise documentation, coordination of logistics, and selection of an evaluation and improvement methodology.

Exercise Objectives

Exercise objectives are the cornerstone of exercise design and development. Exercise objectives define specific goals, provide a framework for scenario development, guide development of individual organizational objectives, and supply exercise evaluation criteria. Planners should ensure objectives are simple, measurable, attainable, realistic, and time-oriented (SMART). The number of exercise objectives should be limited to facilitate design of a reasonable scenario, enable timely exercise execution, and adequately support successful completion of exercise goals.

Identification of exercise design objectives are initially discussed during the concept and objectives (C&O) meeting and confirmed no later than the initial planning conference (IPC). The selection of exercise design objectives is inherently linked to the systems that will be employed and the tasks that will be performed during an exercise. These systems and tasks comprise the capabilities that will be evaluated during an exercise. Once identified, exercise objectives should be linked to one or more of the five prevention core capabilities. *See the Target Capabilities List (TCL) for detailed descriptions of capabilities in the Prevention mission area*.

Exercise Duration

Operations-based prevention exercises are unique in that they may require an extended duration of exercise play, as dictated by the defined exercise scope (i.e., type of exercise, exercise objectives, participants, and scenario). For example, a Drill with participation limited to only a State or local fusion center may only require 2 hours of exercise play, where as a Functional Exercise with Red Team incorporating State and local fusion centers, multiple law enforcement agencies, and public/private sector agencies may require 3 weeks to adequately meet all exercise objectives.

A key factor in determining the capability to conduct extended duration exercises is identifying the fine balance of real world work with exercise play. The exercise planning team has to consider the following design elements in order to determine the duration needed to meet the exercise objectives.

- Type of Exercise
- Exercise Objectives
- Participants
- Resources/Personnel
- Logistics
- Finances

Ground Truth

The Ground Truth for a prevention operations-based exercise should provide the scenario timeline, the local threat environment, and detailed background information of the Universal Adversary (UA) threat group, the catalyst(s) of the exercise as it relates to the scenario. The scenario should be realistic, plausible, and challenging; however, designers should ensure the scenario is not so complicated that it overwhelms participants. The exercise planning team must identify the kinds of player activities that need to be demonstrated to meet exercise objectives, and then ensure that those activities can take place within the Ground Truth framework. *See HSEP Vol IV Controller and Evaluator Handbook for a sample Ground Truth.*

Realism/Threat. The exercise planning team should consider previous real-world incidents and existing plans that have been developed for popular local attractions, large venues, and critical infrastructure or key resources. Detailed information should be limited in quality and quantity to reflect real-world uncertainty. Inclusion of superfluous information, or “white noise,” is a variable that should be discussed and agreed upon by the exercise planning team. Designers should be cognizant of any sensitivities surrounding the Ground Truth by avoiding the use of actual names associated with known terrorist groups.

For example, National Planning Scenario (NPS) 12: Explosives Attack – Bombing Using Improvised Explosive Devices (IED) has been modified to incorporate the UA Prologue as it relates to the prevention IED scenario. In this scenario, the UA – represented by El-Zahir, a fictitious network of Muslim extremists, and American Radical Islamist Converts (ARIC), American-born converts and second-generation immigrant Muslims who support global jihad – use improvised explosive devices (IEDs) to target critical infrastructure and/or soft targets. The UA Prologue is a detailed attack scenario predated to include the seven stages of attack planning (i.e., Trigger, Target Parameters, Target research, Specific target selection, Development of an operational plan, Attack, and Post-attack analysis).

The UA Prologue and the NPS can be modified to correspond to jurisdictions’ needs, objectives, and duration of the exercise. Additionally, the NPS are scheduled for UA Prologue modification to facilitate their use with future prevention exercises, and will be released at a later date. *See HSEEP Volume IV for more information on the NPS #12 with UA Prologue.*

Venue/Target. The venue/target selection should be based on the exercise objectives. When selecting an appropriate venue/target, planners should consider findings from a jurisdiction and/or organization's threat analysis and/or buffer zone protection plan (BZPP) to contribute to scenario development. For example, if critical infrastructure and/or soft targets have been identified in previous analyses, the Ground Truth could describe a threat to one of those locations. The target should also be characteristic of facilities/events typically targeted by the selected adversary.

Documentation

Player Notifications. To ensure safety of Red Team and Blue Team, players should be notified of potential engagement in exercise activities through multiple means. Direct notifications that exercise play is occurring should be communicated to law enforcement agencies through law enforcement networks/messages *prior to and throughout* the conduct of the exercise. Player briefings for State and local law enforcement agencies whose personnel have the potential to be engaged as exercise players should also be provided.

Exercise Plan. Exercise Plans (EXPLANs), which are published and distributed prior to the start of an exercise, provide a synopsis of the exercise. In addition to addressing exercise objectives and scope, EXPLANs assign tasks and responsibilities for successful exercise execution. This document is generally intended for use by exercise players and observers. *See HSEEP Volume IV for a sample EXPLAN.*

> *TIP: The EXPLAN for a prevention exercise should contain background information on the adversary in order to simulate the type of knowledge fusion center analysts and other players would normally possess regarding a real terrorist adversary. This background provision creates realism and negates the need for a large number of information/intelligence injects to be delivered during the first hours/days of a prevention exercise. The background information should be limited to open source and/or media-generated information only.*

An EXPLAN typically contains the following sections:

- Purpose/scope/objectives
- Background
- Duration
- Date and time of exercise
- Exercise planning team/control staff organization
- Roles and responsibilities
- Rules of conduct
- General safety requirements
- Red Team safety requirements (when applicable)
- UA background information
- Logistics
- Security and access
- Communications
- Schedule of events
- Maps and directions

Controller and Evaluator Handbook. Controller and Evaluator (C/E) Handbooks supplement

EXPLANs and contain more detailed information about the exercise scenario. They also describe the roles and responsibilities of exercise controllers and evaluators and the procedures they must follow. Because the C/E Handbook contains the Ground Truth exercise administration, it should be distributed to only those individuals specifically designated as controllers or evaluators. *See HSEEP Volume IV for samples of a C/E Handbook and EEGs.*

In addition to containing information similar to that of the EXPLAN, the C/E Handbook usually contains the following sections:

- Ground Truth
- Roles and responsibilities of individual controllers and evaluators
- Exercise safety plan
- Controller communications plan
- Exercise Evaluation Guide (EEG) data collection forms

Red Team Handbook. If an operations-based prevention exercise makes use of Red Teams, an additional exercise document, the Red Team (RT) Handbook, must be developed. The purpose of the Red Team Handbook is to aid Red Team safety controllers and Red Team controllers/operatives in the conduct of safe and valuable Red Team exercise activity. The handbook provides essential information, not included in any other exercise documents, to Red Team controllers enabling them to understand their roles and responsibilities in exercise execution, and successfully coordinate and direct the Red Team activities during exercise play.

The Red Team Handbook supplements the C/E Handbook and the EXPLAN and contains more detailed information about the Red Team, its planned operations, and the UA it is built to physically represent. Because the Red Team Handbook contains information about the UA, it should be distributed to only those individuals specifically designated as controllers, evaluators, and Red Team operators. *See HSEEP Volume IV for samples of a RT Handbook.*

In addition to containing information similar to that which is in the EXPLAN, the Red Team Handbook usually contains the following sections:

- Ground Truth

TIP: UA dossiers should include a full description of each Red Team operator (e.g., name, aliases, birth date/place, height, weight, build, hair, eyes, markings, complexion, training, known associates, known travel, background, other) with photo and mug shot photo.

- Red Team operational safety requirements
- Detailed description of each Red Team operation (including operation objective, situation, execution date, administration and logistical considerations, and operation-specific safety requirements)
- Target Information (including target location, description, and maps/directions). Target information should be developed by the Red Team operatives using ONLY open-source information
- Red Team operational communications plan
- Example of the Red Team unique identification

Master Scenario Events List. A MSEL contains a chronological listing of the events that drive exercise play. The MSEL links simulation to action and reflects each incident or activity that will prompt players to implement the policy or procedure being tested. MSEL entries are called injects. An event may be injected via player action or controller simulation. Each MSEL inject contains:

- Designated scenario time
- Real-time delivery time
- Event synopsis
- Controller responsible for delivering inject, with controller/evaluator special instructions (if applicable)
- Expected action (player response expected after a MSEL inject is delivered)
- Intended player (agency or individual player for whom the MSEL inject is intended)
- Means of delivery (the system through which the inject is delivered, or the system that is being mimicked by an inject)
- Notes section (for controllers and evaluators to track actual events against those listed in the MSEL, with special instructions for individual controllers and evaluators)

Exercise Evaluation Guides. The HSEEP series of tools includes Exercise Evaluation Guides (EEGs) to help with exercise evaluation. These guides outline and provide guidance on assessing the performance objectives to be accomplished for each capability being tested by an exercise. They were developed by experienced exercise evaluators and practitioners who are subject matter experts (SMEs) to be easily understood and used by evaluators with varying levels of experience. Each EEG provides evaluators with information on what tasks they should expect to see demonstrated, space to record their observations, and criteria to consider after the exercise (as the first step in the analysis process).

Each EEG can be used by one individual evaluator assigned to observe individual performance objectives or groups of performance objectives. During the analysis phase, evaluators combine their observations with those of the other evaluators. They reconstruct events and analyze outcomes and interactions across agencies, organizations, disciplines, and jurisdictions to evaluate the broad capability outcomes. *See HSEEP Volume III for more information on evaluation methodology, and HSEEP Volume IV for sample EEGs.*

Additional Documentation for Large Scale Exercises. Evaluation planning is an important concept for every exercise planning team to address. Reflective of this, during larger, more complex exercises, planners may develop a written Evaluation Plan (EVALPLAN) in lieu of, or in addition to, a C/E Handbook. An EVALPLAN provides evaluation staff with guidance and instructions on evaluation or observation methodology to be used as well as essential materials required to execute their specific functions. The EVALPLAN is a limited distribution document that evaluators use in conjunction with the EXPLAN and the MSEL. *More information on the EVALPLAN and the evaluation process can be found in HSEEP Volume III.*

Likewise, Control Staff Instructions (COSIN) may be employed in lieu of, or in addition to, a C/E Handbook for larger, more complex exercises that require more coordination among control staff. A COSIN contains guidance that controllers, simulators, and evaluators need concerning procedures and responsibilities for exercise control, simulation, and support. In addition to the functions of a C/E Handbook, a COSIN provides guidelines for control and simulation support and establishes a management structure for these activities.

Procedural Flows (PROFLOWs) outline a sequential flow of actions anticipated from participating organizations in response to a hypothetical situation. Typically, they are produced for national- and international-level exercises to describe the procedures of departments and agencies that may or may not be published elsewhere. The PROFLOW is used in conjunction with the MSEL to allow controllers and evaluators to track and monitor expected actions to ensure their completion at designated times. The PROFLOW differs from the MSEL in that it contains only expected player actions and not controller-delivered injects. *Sample EVALPLAN and COSIN are available in HSEEP Volume IV.*

Controller and Evaluator Packets. Prior to an exercise, controllers and evaluators should receive the materials that they need to carry out their responsibilities. These materials can be extracted from the more detailed information found in the C/E Handbook.

A controller packet should contain:

- Essential C/E Handbook information
- MSEL, including injects for each responsible controller
- Relevant target / operational area information

An evaluator packet should contain:

- Essential C/E Handbook information
- MSEL, including injects for each responsible evaluator
- EEGs
- Relevant target / operational area information

These materials should be placed in a packet, folder, or notebook for ease of use during the exercise.

Exercise Site Management

Operational Area. The operational area is the site or facility where the bulk of the intelligence gathering, analyses, and sharing are conducted. As such, this is where the majority of the evaluation of critical tasks will occur as well. This may be a regional intelligence fusion center or other such intelligence gathering facility. In large scoped prevention exercises, multiple operations areas may be necessary. If Red Team play is an element of the exercise, additional operational areas must be specifically delineated to accommodate their activities as well as any corresponding Blue Team activities.

Registration Area. No unauthorized personnel should be allowed into an operations-based exercise site; everyone associated with the exercise should register. All individuals should register immediately upon arrival at the exercise site and receive a badge.

Observer/Media Area. The sensitive nature of a prevention exercise may preclude the invitation of observers and media; however, if invited, they should be directed to a designated area that provides them with a view of exercise play but prevents them from interfering with exercise play or viewing any sensitive material.

Simulation Cell. The Simcell is a working location for a number of qualified professionals who portray nonparticipating organizations, agencies, and individuals who would likely participate actively in response to an actual event. Depending on the type of exercise, the Simcell may require a phone, fax machine, computer, e-mail account, or other means of communication. In prevention exercises, the Simcell may require additional access to specific intelligence or information sharing networks or formats, or a reasonable facsimile thereof, in order to realistically portray the many agencies or departments involved in the gathering, analyzing, and sharing of information, and accurately reflect the information sharing environment in general.

The prevention mission area involves many agencies, departments, and organizations from every level of government working together. For example, the Homeland Security Operations Center (HSOC) is made up of representatives from 35 federal agencies. With such a large number of potential players involved, it reasonable to assume that most will not be included as actual players in the majority of prevention exercises. Therefore, it is essential that the Simcell for prevention exercises be adequately staffed with knowledgeable personnel who can realistically simulate the large number of agencies, organizations, and departments who are not playing. As a result, the Simcell for prevention exercises may need to be larger and contain more persons with specialized knowledge than those utilized in response-oriented operations-based exercises.

Media/Public Information

Public Information/Press Release. The exercise planning team may or may not decide to notify the media of the proposed exercise. This notification can prevent public confusion on the day of the exercise and can assure the public that the community is working to prepare for real-world incidents. The agency/organization sponsoring the exercise should decide whether to invite the media. If invited, the media should have an opportunity prior to the exercise to conduct interviews with key planners and participants.

Either way, prior to the exercise the exercise planning team, working in cooperation with the local public information officer should develop a written release to be disseminated to media outlets in case information is leaked to the media. This release informs the media, and thereby the public, about general exercise information. Prior to an operations-based exercise, it is particularly important to release information about exercise activities that may impact the public or cause citizens to believe an incident has actually occurred. Additionally, this information can be distributed to observers and senior officials. The document should *not* contain detailed scenario information, such as the hazard or venue, or any information that could hinder exercise outcome if read by a participant. *See HSEEP Volume IV for a sample public information/media release.*

Typically, the contents of an exercise public information/press release should include:

- Introduction, including sponsor and exercise program information
- Purpose / expected outcomes
- Scope and duration
- General scenario (e.g., location, goals, objectives)
- Participating agencies, grouped by locality and functional area

Public Announcement. The exercise planning team should also decide whether or not to make a public announcement. A public announcement may be a necessary precaution, or it may deflate public confidence and hinder exercise realism. To determine whether a public announcement should be made, consider the following questions:

- Does the observation of an exercise activity by a member of the public have the potential to cause confusion, fear, or disruption of any kind?
- Are objectives tested more effectively if private citizens remain uninformed participants?

Announcements can be made on local television or radio, in local newspapers, through mass mailings or pamphlets, and/or on signs near an exercise operational area. *See HSEEP Volume IV for a sample public announcement.*

Site Logistics

Badging/Identification. For security purposes, all informed exercise participants should wear some form of identification. Although some players may wear their uniforms, all other participants including controllers, evaluators, support staff, and plain clothes players, should be clearly identified. This identification is usually accomplished through a color-coded system of badges. Badges should be distributed before conducting the exercise, usually during registration or briefings. Players should receive information about the forms of identification they will see at the exercise play area and what each color represents.

Red Team operators should not wear their badges in plain view during a physical Red Team operation. Physical Red Teams should be issued unique identification to present to Blue Team players immediately upon request. *For more information on Red Team unique identification, see Appendix B of this manual.*

Water/Food. Due to the extended duration of most prevention exercises it is recommended that the exercise planning team communicate to all exercise participants in all exercise locations whether food will be made available. At a minimum, water should be available to all individuals present during exercise conduct.

Controller Communications. The exercise planning team should define a controller communications network that will enable controllers, evaluators, and Red Teams to communicate throughout the exercise. The controller network will also allow exercise staff to communicate universal changes in exercise documentation, such the MSEL. The controller network should be managed at the Simcell. An exercise controller phone book, listing controller and evaluator names, contact number(s), and locations should be made available to all controllers and evaluators. The controller phonebook should be published separately from other major exercise documentation and kept confidential.

During extended duration exercises, a daily conference call should be scheduled to communicate important updates to controllers, evaluators, and as appropriate, Red Teams. All available members of the exercise planning team should attend. The following are suggested topics for the daily conference call:

- Report Unusual Events/Safety Concerns
- Debriefs, as appropriate
    - Red Team (Note: Red Team representatives should be excused from the call following their debrief to maintain the firewall)
    - Blue Team
    - Lead Evaluator
    - Simcell
- Follow-up on Previous Action Items
- Action Items
- Next Day's Events

TIP: Red Teams participation should be limited on this conference call to only the Red Team Operations Lead and Red Team Liaison. Red Team daily debriefs should be conducted first and Red Team operators should be excused from the daily conference call following their debrief to avoid any incidental discussions of Blue Team actions.

Videotaping. Because of security concerns, it is important for the exercise planning team to determine which parts of an exercise (e.g., Red Teaming), if any, will be videotaped.

Site Security. Because of the sensitive nature of exercises, and because exercises themselves may become targets, it is important for the exercise site to be secure. Local law enforcement should provide site security.

Weapons Policy. All exercises should employ a written weapons policy that has been approved by senior officials prior to exercise conduct. Operations-based prevention exercises have the potential to garner participation from on-duty law enforcement. For this reason, it may be impossible to inspect and clear weapons prior to activity in the exercise operational area as performed during response-focused exercises.

Red Team operators should be prohibited from carrying weapons of any kind – real or simulated. This policy should be confirmed and documented within the Red Team Rules of Exercise Play, to which all exercise participants are subject. *See HSEEP Volume IV for sample Rules of Exercise Play*.

Safety. Safety is one of the most important considerations in conducting an operations-based exercise. The following safety issues should be addressed:

- Identify a Safety Controller (not to be confused with a Safety Officer designated by IC)
- Identify real-world emergency procedures with a code word or phrase
- Identify safety requirements and policies
- Consider other safety issues outside the scope of exercise control (e.g., Red Teaming, weather, heat stress, hypothermia, fire/pyrotechnics, weapons, animals/K–9s, use of force)

Conduct

Set-up

Members of the planning team assigned to exercise set-up should arrange to begin their task as many days prior to the event as necessary and reasonably possible, depending on the scope of the simulated environment and the operational areas and/or facilities involved. Set-up entails arranging briefing rooms and testing A/V equipment, placing props and effects, marking the afore-referenced areas and their perimeters, and checking for potential safety issues. On exercise conduct days, all planning team members should arrive several hours before the start time to handle any remaining logistical or administrative items pertaining to setup, arrange for registration, and conduct a communications check.

Exercise Participants

Players. Players are agency personnel who have an active role in preventing terrorist incidents by performing their regular roles and responsibilities during exercise play. Players observe Red

Team activities and receive intelligence/information injects. They convert these observations and injects into an overall threat picture, and attempt to prevent the illuminated attack. Players may be informed (such as when receiving an inject labeled "this is an exercise"), or they may be uninformed (such as when observing Red Team activities in the field).

Friendly Force/Blue Team. All State and local law enforcement, and other non-Red-Team-designated organizations and agencies (e.g., security forces assigned to key targets) are considered friendly forces or Blue Team.

Red Team Operators. Red Team operators are exercise participants who portray the physical entity of the adversary as a Physical Red Team. The primary purpose of a Red Team is to apply knowledge of terrorists' motivations, organization, targeting, tactics, techniques, procedures, and equipment in order to exercise and assess the jurisdictions' ability to prevent terrorist attacks. All activities conducted by Red Team operators are monitored by designated Red Team safety controllers.

Controllers. Controllers are exercise participants who plan and manage exercise play, set up and operate exercise venues, and act in the roles of individuals and agencies not actually playing in the exercise. Controllers provide key data to players and may prompt or initiate certain player actions to ensure exercise continuity. *Controllers are the only participants who will provide information or direction to the players.* Controllers may compress exercise time or employ jumps in the timeline to ensure exercise continuity and completion. All controllers are accountable to the senior controller. A controller may also serve as an evaluator.

Evaluators. Evaluators are chosen from various agencies to evaluate and comment on designated functional areas participating in the exercise. Evaluators are chosen based on their expertise in the functional area(s) they will review during the exercise. Evaluators have a passive role in the exercise and only observe and record the actions of players; they do not interfere with the flow of the exercise. Following the end of the exercise, evaluators participate in analyzing the data they have collected and contribute to the development of the AAR.

Briefings

Held prior to an exercise, briefings educate participants about their roles and responsibilities. By scheduling separate briefings for controllers and evaluators, Red Team participants, and players, both onsite and offsite, planning team members can avoid giving extraneous material to different groups. If the exercise planning team has enough members, many of these briefings may be scheduled simultaneously to prevent delay of the exercise start time. Presentations should accompany most of these briefings.

Controller and Evaluator Briefing. The C/E briefing is generally conducted the day before an operations-based exercise. It begins with an exercise overview and then covers areas of operation, schedules of events, scenario, control concept, controller and evaluator responsibilities, ROEP, and any miscellaneous information. This briefing generally lasts 1 to 2 hours. *See HSEEP Volume IV for a sample C/E briefing.*

Player Briefing. A player briefing should be provided to all informed players. If players handling intelligence/information injects will receive any scenario background information, the player briefing is an ideal time to provide it. The remainder of the briefing should cover areas of operation, schedules of play, criteria for evaluation, and most importantly, safety and ROEP. The duration of a player briefing is dictated by several factors, including whether Red Team activities will be conducted, and whether the participants have experienced a prevention-focused exercise in the past.

Exercise Play Rules

Exercise play rules establish the parameters that participants will follow. These rules help players understand their roles in the exercise environment, enabling the tasks they perform to be effectively evaluated. These rules also describe appropriate behavior, establish guidelines for physical contact, and aim to prevent physical harm to individuals or damage to property. Written rules must be provided in advance to all parties. These rules should first be reviewed and approved by appropriate authorities.

Wrap-up Activities

Debriefs subsequent to the end of the exercise provide an opportunity for controllers, evaluators, and players to review general exercise proceedings.

Player Hot Wash. A hot wash is led by a controller in each functional area immediately following the exercise and allows players to provide immediate feedback. It enables controllers and evaluators to capture information about events while they are still fresh in players' minds. The hot wash is an opportunity to ascertain the level of satisfaction with the exercise, identify issues or concerns, and propose items for improvement.

Players should complete and submit their feedback forms during the hot wash. All evaluators will take notes for later compilation during play and hot washes in their functional areas. Information from the participant feedback forms will be used to help generate the After Action Report (AAR). Attendance lists will be collected and secured by the lead exercise planner. *See HSEEP Volume IV for sample feedback forms.*

Controller and Evaluator Debrief. The C/E debrief provides a forum for functional area controllers and evaluators to review the exercise. This session is a discussion facilitated by the lead exercise planner during which each controller and evaluator has an opportunity to provide an overview of the functional area they observed, including strengths and areas for improvement. During the debrief, controllers and evaluators should complete and submit their EEG data collection forms and analysis forms as well as their participant feedback forms. Debrief results will be captured for inclusion in the AAR. *See HSEEP Volume IV for a sample C/E debrief.*

Specific Exercise Types

Drills

A drill is a coordinated, supervised activity usually employed to validate a specific operation or function in a single agency or organization. Drills are commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills. Drills are narrow in scope and typically focus on a specific aspect of an operation. For example, intelligence centers may drill on the production of intelligence reports and their dissemination to appropriate stakeholders with varying levels of clearance and need using one or several communication channels. Drills can be used to determine if plans can be executed as designed, to assess whether more training is required, or to reinforce best practices. In addition to being a valuable stand-alone tool, a series of individual drills can also be useful in preparation for a larger exercise. For example, a series of drills can be used to prepare several agencies/organizations to collaborate in preparation for an upcoming FE with Red Team.

Typical attributes of drills include:

- Narrow focus, results measured against established standards
- Instant feedback
- Realistic environment
- Performance in isolation
- Preparation for exercises that are larger in scope

For every drill, clearly defined plans, policies, and procedures need to be in place. Personnel need to be familiar with those plans and policies, and to be trained in the processes and procedures to be drilled.

A drill may start with brief remarks by the lead exercise planner. Once controllers and evaluators are properly stationed, the drill begins. If no safety issues arise, the drill continues until the process is complete, time expires, or objectives are achieved. During the event, participants must know that they are participating in a drill and not an actual event.

Controllers ensure that participant behavior remains within predefined boundaries and that entities not involved in the drill are not unnecessarily mobilized. Evaluators observe behaviors and compare them against established plans, policies, procedures, and standard practices (if applicable). Safety controllers ensure all activity takes place within a safe environment.

Functional Exercises

FEs, also known as command post exercises (CPXs), are designed to test and evaluate capabilities, multiple functions and/or subfunctions, or interdependent groups of functions. FEs focus on exercising plans, policies, procedures, and the staffs involved in management, direction, command, and control functions. FEs simulate the reality of operations in a functional area by presenting complex and realistic problems that require critical thinking, rapid problemsolving, and effective response in a highly stressful environment.

Notional events are projected through an exercise scenario with event updates that drive activity at the management level. The information/intelligence comprising the events of a FE is handled in a realistic, real-time manner; however, it may represent information/intelligence spanning a period of time longer than that of the exercise's real-time length. For example, while the duration of the FE may be 21 days, the intelligence/information input may represent intelligence/information dating back one year prior to the exercise date. In an FE, movement of personnel and equipment outside of the exercise site is simulated.

Prevention FEs are generally focused on exercising the specific plans, policies, procedures, agreements, networks, and staffs of fusion centers or law enforcement agencies with counterterrorism missions. Adversary actions are largely simulated and delivered in the form of shared intelligence; however, some adversary actions may be carried out by Red Teams in a separate but coordinated category of exercise play.

Typical FE attributes include:

- Performance analysis
- Management evaluation of fusion center/counterterrorism department staff
- Inspection of established policies and procedures that pertain to the scenario

- Measurement of capability
- Examination of cooperative (e.g., inter-jurisdictional) relationships/agreements
- Use of a MSEL as the primary tool that drives exercise play

To create an effective environment, the exercise planning team should represent the real world with respect to potential areas of play. This is accomplished through employment of a Simcell and a highly developed MSEL that incorporates expected player actions and information needs. Agency/organization and player actions must be anticipated, and information resources to match these actions must be identified and assembled. As with other types of operations-based exercises, the exercise planning team must ensure that entities not involved with the exercise are not unnecessarily mobilized.

Briefing and training of controllers and evaluators should be accomplished prior to the exercise date. This briefing and training should be long enough to allow for questions and a visit to the exercise site. Controllers and evaluators should be able to meet each other and determine where they will be located during the exercise. Controllers should be briefed on their responsibilities and the ROEP, and evaluators should become familiar with exercise objectives, EEGs, and the reporting process. Controllers and evaluators should find positions for themselves where they can observe actions but avoid impeding exercise play. During the FE, participants must know that they are participating in an exercise, not an actual incident.

FE controllers use a MSEL to ensure participant behavior remains within predefined boundaries. Controllers in the Simcell will inject scenario elements to simulate real events. Evaluators will observe behaviors and compare them against established plans, policies, procedures, and standard practices (if applicable), as well as against the timeline set forth in the MSEL. Safety controllers will ensure all activity takes place within a safe environment.

Depending on their scope, prevention FEs may require longer exercise duration (several days or weeks) than response-focused FEs in order to adequately evaluate the selected capabilities. Although the exercise may have a time limit, it is best if the end of the exercise occurs after exercise objectives have been met and all required functions are completed to the satisfaction of the lead exercise planner and/or the exercise planning team.

Evaluation and Improvement

See HSEEP Volume III for more information on operations-based exercise evaluation and improvement.

Appendix A

Analytical Red Teaming

Analytical Red Teaming uses an adversary perspective to advance security by providing an alternative view of threats, vulnerabilities, and countermeasures. Without testing the physical limitations of antiterrorism measures analytical red teaming can offer insight to challenge prevailing views, prevent surprise, help allocate resources, and expand the bounds of imagination. Analytical Red Teaming may occur as part of a discussion-based exercise (e.g., TTX) or as a stand-alone activity. This process indoctrinates participants into the mind-set of a specific adversary, modeled upon the results of the threat analysis. Once this perspective has been viably gained, participants use it to build a threat or attack that assaults the plan(s), policy(s), or procedure(s) under examination. Analytical Red Teaming may be conducted by agencies/organizations possessing any level of capability, at a lower cost and shorter time commitment than physical Red Teaming.

Red Team Background

Historically, the concept of Red Teaming has been used for various purposes, including:

- peer review of a plan or procedure;
- assessing vulnerabilities of structures and/or perimeters;
- assessing vulnerabilities of systems, especially within the information-warfare arena;
- testing of security systems, especially by replicating the tactics of a specific adversary;
- producing a credible and realistic representation of actual events and outcomes; and
- defining a threshold of detection, suspicion, and action.

Red Team activities can provide added benefit to a prevention exercise by increasing participants' awareness of the tactics, techniques, and procedures employed by terrorists and criminals unique to the geographical areas in which exercises are conducted. Prior to conducting Red Teaming of any kind, the exercise planning team should conduct a threat analysis to ensure realistic representation of the hazards posed to the personnel, procedure, and/or target being exercised.

Analytical Red Team participants may include both indoctrinated Red Team portrayers and exercise players discussing their real-world duties and decision making processes. Alternatively, one group of participants may analyze the planning and tactics of both Red and Blue actions in consideration of a given scenario. Depending on the needs and resources associated with a planned exercise, a sliding scale of options for exploiting the benefits of the Analytical Red Team methodology can be considered.

Characteristics of an Effective Red Team Activity

Planners and facilitators of Analytical Red Teams must be able to capture the adversary's culture and presenting a realistic challenge to exercise participants, without compromising actual intelligence. For this purpose, HSEEP recommends representing current and real terrorist threats in prevention exercises through the Universal Adversary (UA). The UA models are maintained by the Department of Homeland Security (DHS) and define the terrorist threat in terms of motivation, capability, and intent. The UA is a fictionalized terrorist group that is represented by the Red Team. DHS is able to provide detailed descriptions of each UA threat, including group profiles, individual terrorist background information, and technical data on conventional and improvised weapons.

Threat/Adversary

Analyze Local Threat Situation

In a prevention exercise, local or regional intelligence background information serves as the foundation for the development of the UA and exercise scenario. It is essential that the exercise participants are presented with a realistic threat so that the plans, policies, and procedures in place to defend against it are accurately tested.

UA Development. Generally, open source information can be monitored or reviewed to determine the type of threat most imposing upon a jurisdiction. Law enforcement sensitive records can also provide substantial information on individuals, incidents, and trends; however, exercise planners should limit its use to avoid inadvertent circulation in exercise documentation. The information collected should be compared with the DHS UA profiles. Once a similar profile is selected, it should be customized for accuracy in comparison with the jurisdiction's geographic area and the infrastructure located within it. The aspects of the UA that are of most importance are the UA's ideology, motivation, tactics, capability, and objectives. It is important to note when developing the UA for the exercise that while the UA should represent realistic threats to the jurisdiction, it should in no way compromise actual intelligence.

Scenario Development. The purpose of the scenario is to provide the Analytical Red Team a basis on which to formulate their plan of attack. The scenario is developed by the exercise planning team and should not be a detailed script of an attack, but rather a general outline that provides the Red Team the parameters within which to operate. Much of the information provided in the exercise scenario is determined or driven by the UA profile being used for the exercise. Because of this the exercise planners must ensure that all elements of the proposed attack match the UA profile. The following represent common scenario variables for prevention exercises:

> ***UA Profile*** – The UA profile provides detailed background information on the group being portrayed. Most importantly to scenario development, this includes the typology, ideology, motivation, tactics, capability, and objective of the group. The UA profile is the most important facet of the exercise scenario as every other variable must be in keeping with it.
>
> ***Objective*** – This refers to the objective(s) of this particular operation, not the broader objective of the UA group. The operation objective is an important feature of the scenario as it will largely determine the target, location, and weapon of the operation. For example, if the objective is to attack and destroy the federal government, targets could be symbolic government institutions, with the location of the State capitol building, using a VBIED as a weapon. Alternately, if the objective were to damage the U.S. economy, the target would be the economic system in general, with the specific location being the New York Stock Exchange, using a cyber attack.
>
> ***Target*** – The target of the operation refers to in broad terms who or what the group is to attack. Targets are generally divided into four categories: military, economic, symbolic, and pedestrian (civilians). This should be chosen by the exercise planning team and

should be in line with the operation's objective and the UA profile. Given their breadth, there may be a significant degree of overlap between the target categories. Within these broad categories of targets, the Analytical Red Team is given great leeway to further specify their target. The target selection is the primary determinant of the location for the attack.

Weapon – Largely dependent on the scenario objective, target, and especially the UA's capability and tactics, this refers to the broad category of weapon employed in the attack and is determined by the exercise planners. Weapons may be chemical, biological, radiological, nuclear, explosive (CBRNE), cyber, conventional weapons (e.g., firearms), or a combination of one or more. The exercise planning team should further specify the actual agent (e.g., smallpox, ANFO VBIED, sarin, cesium RDD) and provide accompanying information on the weapon to Analytical Red Team participants. The exercise planning team may also choose to select the specific method of delivery of the weapon, or leave this matter to the discretion of the Red Team. This will largely depend on the exercise or program objectives which may require that a particular method, such as a VBIED be employed. The weapon employed will impact the target location that is chosen.

Location – Unless specifically identified by the exercise planning team to facilitate exercise or program objectives, the actual location or locations of the theoretical operation should be determined by the Analytical Red Team in accordance to their given target. The only requirements are that the location(s) must be within the jurisdiction in which the exercise is being conducted and that its selection accurately facilitates the evaluation of exercise objectives.

With these general parameters of the scenario outlined, the details of the scenario, such as plans for attack and escape, communications, and logistics are to left for the Analytical Red Team to determine during the course of the exercise. These details must remain consistent with the character of the UA group being portrayed. This is achieved through a focused indoctrination of the Analytical Red Team participants (*see* Indoctrination, *below*).

An example scenario outline could be presented as follows:

UA Profile: Religious terrorists dedicated to the destruction of the U.S.

Objective: Inflict maximum casualties on the enemy (U.S.)

Target: Pedestrian (civilians)

Weapon: Explosives (ANFO VBIED)

Location: To be chosen by Red Team (e.g., metropolitan area mass transit system, mass gatherings/celebrations, night club, shopping mall)

Exercise Design Requirements for Analytical Red Teams

Identify Scope of Red Team Activities

Purpose. Red Team activities should prompt decisions and efforts by senior officials to establish new, or improve existing plans, policies, and procedures to prevent terrorist attacks.

Objectives. Red Team activities should produce analysis and evaluation of current plans, policies, and procedures intended to prevent terrorist attacks. Activities will probe for and exploit weaknesses or gaps in the current prevention efforts.

Concept. The exercise planning team should identify a concept of Red Team activities that will facilitate the achievement of exercise objectives. This concept of activities is reflected in the exercise planning team's construction of the exercise scenario (*see* Scenario Development, *above*).

Participants. All persons invited to participate in the discussion-based exercise by the exercise planning team will participate as part of the Analytical Red Team. No specialized background or previous training is required for these individuals to serve as Analytical Red Team members, only that they have strong working knowledge of their own jurisdiction or agency's plans, policies, and procedures. In this way, they are the same as any other discussion-based exercise participant.

The exercise planning team must also identify personnel to be responsible for the indoctrination of the Analytical Red Team participants, assist in the development of their plans of attack, and facilitate discussion of the attack plans (*see* Choose and Expert, *below*).

Choose an Expert

An appropriate expert on the threat represented in the UA must be involved in the Analytical Red Teaming process. This individual should have an operational, academic, and most importantly ideological understanding of the portrayed adversary. The expert should be an enthusiastic public speaker, an experienced leader, and have the ability to develop realistic scenario elements as play unfolds. The adversary expert's responsibilities in the development and execution of Analytical Red Team activities include the following:

- Develop or modify the UA profile for the exercise, if necessary.
- Participate as part of the exercise planning team in the development of the exercise scenario to ensure it is in keeping with the ideology, objectives, capabilities, and tactics of the UA.
- "Indoctrinate" Analytical Red Team participants (*see* Indoctrination, *below*)
- Assist Analytical Red Team participants as they develop plans of attack by answering questions concerning the UA's ideology, objectives, capabilities, and tactics. In this role the expert also serves to keep Red Team participants' plans within the proscribed scenario parameters and consistent with the UA profile.
- Facilitate the discussion of Analytical Red Team plan(s) of attack, highlighting important points, features, and issues. In this function the expert will not serve as a judge to grade the plans as good or bad, but rather will operate as any other SME facilitator to stimulate further thought and prompt discussion.

Analytical Red Team Conduct and Evaluation

This section reflects the elements that must be conducted or included in order to successfully incorporate Analytical Red Team activities into an exercise.

Indoctrination

Analytical Red Team participants will study the UA profile and scenario parameters of the exercise. First, they must be indoctrinated into the UA group, absorbing its ideology, motivation, objectives, and capabilities. This indoctrination is guided by the adversary expert, who uses his/her subject matter expertise to familiarize the Red Team participants with the broad concept of terrorism and specific features of the UA model. The purpose of the indoctrination is to engender in the Analytical Red Team participants the appropriate terrorist approach/mindset required for their role in the exercise. The areas most important to stress in the indoctrination process are:

- Foundation – the basics of terrorism: its purpose, the terrorist mindset
- UA ideology – the driving belief(s) of the UA group in the exercise
- UA motivation – the reason(s) for attack
- UA capability – the skills, abilities, and resources of the UA group to conduct the exercise operations and attack
- UA objective – the intended or desired outcome(s) and effect(s) of the attack
- UA tactics – the method(s) of operation and attack employed by the group

More specific information that should be considered for use in indoctrinating Red Team participants may include the following:

- Group composition
- Political, religious, social, or ideological aims
- Objectives
- Motivations
- Command-and-control structures
- Operational organizations and external ties
- Internal and external support structures
- Headquarters, areas of operations
- Fronts and alliances
- State and government ties
- Training
- Tactics and operations
- Attack methodology
- Key operational considerations
- Decision-operation cycle
- Logistics
- Financing
- Ties to criminal activities
- Weapons and ammunition
- Combat effectiveness
- Key personnel
- Culture
- Threats to U.S. Homeland
- Group background and history

The indoctrination should make use of print and multimedia materials to facilitate the rapid transfer of knowledge to the Analytical Red Team participants.

Plan of Attack

Plan of attack development is the crux of the Analytical Red Team activities in discussion-based exercises. It is this plan or plans that will identify the strengths and/or weaknesses of the current plans, policies, and procedures for terrorism prevention. Development of the plan of attack is left to the Analytical Red Team participants, who will use their own knowledge of existing prevention efforts, the provided attack scenario outline, and their knowledge of the UA.

TIP: The exercise planning team may also choose to provide an attack tree that has been scrubbed of specific details to the Red Team participants. The attack tree serves as a roadmap or guide to the options, actions, and decisions involved in carrying out a terrorist attack. This may expedite plan of attack development, but will often reduce the creativity of Red Team participants as they will tend to follow the options on the attack tree instead of developing imaginative, new ways with which to test the current terrorism prevention plans, policies, and procedures.

Depending on the size of the exercise or preference of the exercise planners, the Analytical Red Team participants will either develop their own individual plan of attack or be grouped into small "cells" to develop a joint plan of attack. If Analytical Red Team cells are formed, exercise planners should limit the size of these groups to no more than 8 individuals, and provide a facilitator for each. When choosing how, or if, to divide the Red Team participants into cells, it must be remembered that each plan of attack will be analyzed individually during the second half of the exercise. Therefore, it is essential to balance the number of attack plans produced (by limiting the number of cells or individuals) in order to afford each adequate time for examination and analysis.

TIP: When conducting an exercise that includes a large number (5 or more) of Analytical Red Team cells, it is often beneficial to assign slightly altered scenarios to each, or a number of, the cells in order to maintain interest and reduce monotony (e.g., change the target, tactic, or weapon).

Construction of the Red Team plan of attack is facilitated by leading the Analytical Red Team participants through the steps, actions, and decisions that must be made of a terrorist attack, as well as the considerations that are made for each. This is achieved by the expert and/or facilitator asking leading questions to the Red Team as they develop their plan to attack. Examples of such questions are:

- How will you obtain the weapon/materials?
- How difficult to obtain is the weapon/materials?
- Where will you store the weapons/materials?
- How will you transport the weapons/materials?
- Do you need any special equipment or knowledge to obtain/create, transport, handle, or store it?
- What is your target?
- How vulnerable is the target?
- What method of attack will you use?
- When will you attack?
- How will you communicate with other members of your group/cell?
- How will you avoid detection?
- How does this operation meet the overall objectives of the group?
- What is your infiltration and/or escape plan?
- How many members are needed to conduct this attack?
- What special skills are needed to conduct this attack?
- How much will the operation cost?
- How will you fund it?

Analysis

Following the completion of the plans of attacks, participants will cease operating as an Analytical Red Team and examine, discuss, and analyze the terrorist plans. The following important questions should be answered by this examination process:

- What are the key decision points in the operation?
- What are the critical vulnerabilities in this attack plan (where can it be disrupted)?
- What possible evidence or signatures will any of the decisions or actions produce?

Once these questions have been answered, exercise participants should walk through the plan(s) of attack step by step. At each step exercise participants should assess how, or if, their current plans, policies, and procedures for terrorism prevention could detect and/or disrupt the terrorist activities. If current terrorism prevention efforts display limited or no ability to do so, steps should be taken to develop plans, policies, and procedures that seize upon the potential signatures made by terrorist planners and focus on the critical points of terrorist attack plans. These new plans or improvements to existing ones should begin their initial development at the exercise utilizing the input from the assembled players.

These observations and assessments should be captured for inclusion in the AAR. Copies of the Analytical Red Team plan(s) of attack should be collected and included as well.

Appendix B
Physical Red Teaming

Physical Red Teaming involves individuals portraying realistic adversary moves and countermoves an exercise. A Physical Red Team embodies the selected UA and its cell members, acting according to the group's motivations, capabilities, and intent. Red Team operators create opportunities for Blue Team to prevent the ultimate attack as the operators plan, prepare, and leave signatures. On a sliding scale of levels of realism, they act out the execution of steps dictated by known terrorist tactics, techniques, and procedures, providing a means for the Blue Team players to interact with the adversary in an exercise setting.

Red Team Background

Red Team activities can provide added benefit to a prevention exercise by increasing participants' awareness of the tactics, techniques, and procedures employed by terrorists and criminals unique to the geographical areas in which exercises are conducted. Prior to conducting Red Teaming of any kind, the exercise planning team should conduct a threat analysis to ensure realistic representation of the hazards posed to the personnel, procedure, and/or target being exercised.

Operations-based exercises can employ physical Red Teams, also known as Opposing Forces (OPFOR). Physical Red Teams are, by definition, reactive and thinking. They adapt to player decisions and actions according to the prescribed adversary's motivations and tactics, which often provides players with instant feedback. Physical Red Teaming offers the opportunity to engage more participants than Analytical Red Teaming, and to rehearse actual movement of personnel, equipment, and information/intelligence messages. Safety issues must be a primary consideration when conducting Physical Red Teaming.

Characteristics of Effective Physical Red Team

Red Team planners and operators must be able to capture the adversary's culture and presenting a realistic challenge to exercise participants, without compromising actual intelligence. For this purpose, HSEEP recommends representing current and real terrorist threats in prevention exercises through the Universal Adversary (UA). The UA models are maintained by the Department of Homeland Security (DHS) and define the terrorist threat in terms of motivation, capability, and intent. The UA is a fictionalized terrorist group that is represented by the Red Team. DHS is able to provide detailed descriptions of each UA threat, including group profiles, individual terrorist background information, and technical data on unconventional or improvised weapons.

To be effective, Red Team operators should demonstrate understanding of the selected UA group and individuals whom they are portraying. The operators should study the provided UA profiles to be able to embody their culture, motivations, capabilities, intent, and ideology in the case of player interaction. This effort to remain consistent with group and individual profiles benefits players, as adversary behavior remains consistent and realistic; it also benefits the operators, as it creates an opportunity to test vulnerabilities through the adversary's perspective, much like Analytical Red Teaming.

Effective Physical Red Teams also create abundant opportunities for significant interaction with exercise participants. As determined by the exercise objectives, Red Team actions should cause players to recognize suspicious behavior, investigate networked resources, share information, and/or any number of other steps to preventing the particular attack. When Physical Red Teaming is conducted in concert with other prevention exercise activities, information properly collected and shared by players through interaction with Red Teams can contribute to the information and intelligence used to prompt the drill, functional, or full scale portion of play.

For safety reasons, Red Team operators should NOT attempt to interact with players by driving erratically, physically threatening individuals or gatherings, or provoking a vehicular or foot chase. Examples of appropriate opportunities for interaction include, but are not limited to:

- Suspicious behavior that prompts a private citizen to report it,
- Attempts to purchase weapons or weapon components, and
- Inquiries to private security or law enforcement regarding security measures or structural viability of a potential target site.

Ultimately, an effective Red Team will be able to test narrowly defined elements of the exercising jurisdiction's antiterrorism plans, policies, and procedures through its operations. For this reason, it is recommended that individuals with a detailed understanding of these plans and procedures participate in planning Physical Red Team operations.

Threat/Adversary

Analyze Local Threat Situation

In a prevention exercise, local or regional intelligence background information serves as the foundation for the selection of the UA and its target(s). It is essential that exercising personnel are presented with a realistic threat so that plans and the tasks that comprise them are accurately tested.

UA Development. Generally, open source information can be monitored or reviewed to determine the type of threat most imposing upon a jurisdiction. Law enforcement sensitive records can also provide substantial information on individuals, incidents, and trends; however, exercise planners should limit its use to avoid inadvertent circulation in exercise documentation. The information collected should be compared with the DHS UA profiles. Once a similar profile is selected, it should be customized for accuracy in comparison with the jurisdiction's geographic area and the infrastructure located within it.

Target Selection. Targets may be selected either by the exercise planning team or by Red Team operators after they have been indoctrinated into their adversarial roles. The target(s) should be consistent with 1) the information gathered on the local threat environment, 2) the propensity of the selected UA to attack the given type of facility or event, and 3) the length of time, time of year, and weaponized hazard of the selected exercise scenario. If targets are selected by Red Team operators, the exercise planning team must be informed of them, in order to address logistical planning elements and include them in exercise control documents.

Once a target is selected, it may be helpful to develop a target information packet (TIP). The TIP helps prepare Red Team operators for safe field activities in a given operational area. Similar to target selection, TIP development can be completed either by the exercise planning team, or by already-indoctrinated Red Team operators. The exercise planning team should utilize internal information such as facility blueprints, buffer-zone protection plans, or municipal records to develop a TIP.

Alternatively, the Red Team should use the same targeting methodology a terrorist adversary would use to collect such information. This methodology might include remote targeting (gathering information from the internet or other sources without physically visiting the location), or reconnaissance and surveillance (R&S) of a given target, as a controlled activity in a prevention exercise series.

The essential elements that should be included in a TIP are:

- **Target overview –** the description and significance of the specific target including the following:
    - Target identification data (address, GPS coordinates, phone number, URL)
    - Imagery (visual description, maps, satellite images, photos)
- **Outcome/motivation –** brief description the desired target-specific effects of attack, consistent with the selected UA's motivation, capabilities, and intent. This section may include potential unintended consequences.
- **Detailed target description –** information on operating procedures, history, collocated/adjoining structures/businesses, and previous hazards/threats.
- **Environment –** significant environmental information, including the following:
    - Geographic data (name of city/town and local municipal sites, such as schools)
    - Meteorological data (climate overview for the region)
- **Threat** – information pertaining to the current threat *to the Red Team*, including the following:
    - Paramilitary and indigenous forces (intelligence, security, and police services that could detect and prevent the Red Team)
    - Counterintelligence environment (known efforts to collect information in order to prevent actions by terrorist elements such as the Red Team)
    - Other first responders that could interfere with the operation
- **Demographics and cultural features** – include the following information:
    - Area population characteristics (census data)
    - Ethnic composition
    - Hospitals/medical centers
    - Libraries and Internet cafes
    - Social conditions (median statistics on age, income, home value, education levels, etc.)
    - Religious affiliations and places of worship

- **Lines of communication, information systems, and transit** – include the following information:
    - Airfields, railways, and major roadways
    - Power grid
- **Infiltration and exfiltration** – what local resources can the Red Team exploit to facilitate the attack and potentially escape and evasion? Examples include:
    - Apartment listings for available housing near target
    - Open employment positions within the company that owns or secures the target
    - Chokepoints between insertion point(s) and objective (identification of limited access/egress)
    - Electronic warfare attack tools
    - Analytical tools and references to aid understanding the region, reconnaissance, planning, or the attack
- **Sources used to gather TIP information –** citations to validate the information contained in the TIP, which may be useful for identifying information that is currently public but should be controlled.

Exercise Design Requirements for Physical Red Team Activities

Identify Scope of Red Team Activities

Purpose. Red Team activities should provoke decisions or actions by the public, law enforcement, or security personnel that measure specific exercise objectives. Each Red Team activity should be proposed in a Concept of Operations (CONOP) document, approved, synched with the MSEL, refined, and finally developed into an Operation Order (OPORD) to ensure its purpose is measurable.

Objectives. Red Team activities should provide a means to evaluate selected exercise objectives. In general, exercises provide the opportunity to evaluate performance objectives in a highly controlled environment. To ensure this evaluation is accurate in the case of Physical Red Teaming, operators must be trained to make decisions based upon the terrorist adversary's perspective *(see* Characteristics of an Effective Red Team, *above).*

Concept. The exercise planning team – to include a Red Team Liaison – should identify a concept of Red Team activities that will facilitate achievement of exercise objectives as well as reflect the adversary's planning, preparation, and execution of an attack realistic to the given scenario. These concepts should be developed into a series of operations to be proposed to the core planning team for review and consideration no later than the Midterm Planning Conference (MPC).

These proposals should outline specific activities, the exercise objective each activity is designed to test, the timing of the activity within the notional exercise timeline, and the adversary's basic motivations and tactics. Operations should reflect local threats/vulnerabilities, selected targets, UA profile information, and timing coordination with the MSEL. PHYSICAL RED TEAM OPERATIONS ARE ALWAYS DEVELOPED WITH SAFETY AS THE FOREMOST CONSIDERATION.

Participants. The exercise planning team and Red Team Operations Lead will determine the resources necessary for safe and effective execution of the proposed operations. The exercise planning team will identify individuals to portray UA individuals executing Red Team activities. Each individual will represent a cell member and carry out that member's prescribed functions.

Exercise planners will also identify persons to function as Red Team evaluators and safety controllers. Exercise planning team members make good Red Team evaluators and safety controllers – when not engaged in other conduct roles – because they are familiar with the details of the Red Team operations, and because they have the institutional knowledge necessary to intervene during a potential safety hazard. Ideally, safety controllers will be selected from among sworn law enforcement officers. It is vitally important that safety controllers and evaluators be able to observe the Physical Red Team activities without interfering or drawing unnecessary attention to their presence.

In operations-based prevention exercises where a Physical Red Team is used, a Blue Team is inherently created. The goal of Blue Team participants will be to prevent the Red Team attack from occurring by intercepting or disrupting the Red Team activities through the plans, policies, and procedures being evaluated. Blue Team participants include both informed exercise players (e.g. police officers) and uninformed participants who come into contact with the Red Team members during an event (e.g., members of the public, retail proprietors, security guards).

Determine General Safety Requirements

Safety is the primary consideration when designing Physical Red Team activities. Safety requirements are developed to maximize the safety of exercise participants while preserving scenario realism. This is achieved through the creation of rules of exercise play (ROEP) and issuance of unique identification to operators.

Rules of Exercise Play. The operations branch of the exercise planning team should develop rules of exercise play (ROEP). ROEP provide specific guidance for the behavior of Red Team members, controllers, and informed participants during the exercise. ROEP address numerous issues *(see* Develop ROEP*, below)*, but most importantly the safety of all exercise participants.

The following are some of the possible safety considerations that should be addressed in the ROEP:

- Interaction with law enforcement, private citizens, off-limits individuals, and other groups as necessary
- Use of physical force
- Possession of firearms and weapons
- Activity areas: in- and out-of-play boundaries, use of specific property or infrastructure, jurisdictional considerations
- Apprehension or pursuit of Red Team members by law enforcement or other players
- Personal safety
- Non-player contact (e.g., law enforcement not associated with the exercise, K-9 units, HAZMAT units, other first responders)
- Hazardous environments (e.g., maritime or flight activities)

All exercise participants are responsible for adhering to the operational guidelines and safety requirements defined in the ROEP.

Unique Identification. The potential for interaction between Physical Red Team members and Blue Team law enforcement or security evokes some safety concerns. To avoid any confusion or violations of the safety protocols and/or ROEP in these situations, HSEEP strongly advises each Red Team operator, safety controller, and evaluator carry a unique identification. Examples of unique identification include, but are not limited to:

- A credentialing letter signed by a recognizable official, or
- An encoded exercise badge.

In case of interaction with local law enforcement or security personnel, Red Team participants must follow the appropriate guidance detailed by the exercise's ROEP. In general, when confronted or challenged by a law enforcement officer Red Team participants are instructed to stand down, stop play, identify themselves as exercise participants, present the officer with the unique identification, and follow the instructions of the officer. Red Team operators and evaluators will refer the officer to the Red Team safety controller. When approached, the Red Team safety controller (ideally a sworn law enforcement officer), will identify himself/herself and present official credentials and a unique identification.

The unique identification should contain the following information:

- A point of contact for verification;
- Statement that the person presenting it is a certified member of the Red Team for the named exercise, and that his/her actions or activities are within the confines of that exercise;
- The days/dates of exercise play; and
- Instructions on how to proceed, including a reminder to request personal identification.

The unique identification should be highly controlled and distributed only by the Red Team Operations Leader.

Physical Red Team Planning, Conduct, and Evaluation

This section reflects the planning steps and actions that must be conducted or completed by the exercise planning team, often in concert with the Red Team Operations Leader, in order to successfully plan Physical Red Team activities and incorporate them into an exercise. The steps are presented in chronological order.

Step 1: Develop Red Team Concept of Operations (CONOPS)

Once the Red Team Operations Leader has been identified, he/she will work with the exercise planning team to develop the Red Team Concept of Operations (CONOPS). The CONOPS is the format for the proposal described earlier *(see* Identify Scope of Red Team Activities, *above).* The CONOPS describes the basis and direction for the Physical Red Team exercise activities. The CONOPS contains specific activities, the exercise objective each activity is designed to test, the timing of the activity within the notional exercise timeline, and the adversary's basic motivations and tactics.

Some real-world considerations will affect the CONOPS. Time, budget, and/or safety constraints may necessitate limiting the scope of certain activities. In these cases, planners should consider shifts in timing or scope, which can contribute to the ability of the activity to be carried-out.

The Red Team Operations Leader will work with the exercise planning team to develop the CONOPS. At a minimum, a Physical Red Team CONOPS should include the following:

- Name of the exercise event and mission
- Type of Red Team operation (e.g., R&S, acquisition of weapons)
- Applicable references (e.g., Memoranda of Understanding, exercise directives)
- Background information providing a description of the purpose and scope of Physical Red Team operations
- A brief narrative that outlines, in general terms, the concept for Red Team operations in support of exercise objectives (should answer the questions who, what, when, where, why, and how?)
- Detailed coordinating instructions that delineate roles, responsibilities, and timelines
- Date/time
- Logistics
- Use and ownership of audio and video gathered by the Red Team
- Safety considerations

The CONOPS should be developed based on discussions reviewed following the Initial Planning Conference (IPC), and reviewed no later than the MPC. *See HSEEP Volume IV for a sample Red Team CONOPS.*

Step 2: Develop Rules of Exercise Play (ROEP)

As introduced above, ROEP are essential design elements of Physical Red Team activities. All Red Team operators, safety controllers, evaluators, and informed participants are subject to the ROEP during the exercise. ROEP define the boundaries for exercise play, and establish limits on Red Team activity to avoid interference with critical public safety and venue site activities, ensure that useful information is gathered, and, most importantly ensure the safety of all participants. ROEP should be developed by the operations branch of the exercise planning team, with cooperation from other stakeholders as needed.

Red Team CONOPS should be developed prior to the ROEP, as the CONOPS may necessitate that some activity-specific rules be included. A discussion of the boundaries of each activity is a good method for beginning construction of the ROEP. The following is a framework for discussion, but is not an all-inclusive list.

The ROEP must be presented no later than the MPC, and reviewed shortly thereafter. Following review, the ROEP should be prepared for approval at the third planning conference. Once they are approved all further operation planning and conduct should occur within the established rules. All exercise participants are responsible for adhering to the operational guidelines and safety requirements.

Participants. This section should identify participants and their roles and responsibilities. Participants include Red Team operators, safety controllers, evaluators, exercise players, friendly forces, and people who might come into contact with Red Team operators during an event. Guidelines for contact with each group should be specified. This section should also provide a description of the unique identification that each Red Team participant will be carrying.

Activity-specific safety requirements. This section provides the following information:

- Identification of safety controllers
- Guidelines for how and when safety controllers should intervene
- Reporting and debriefing protocols
- Definition of specific activity areas for each event, including in- and out-of-play boundaries

General. This section contains rules that are applicable for all activities, which ensure that exercise play will not disrupt any of the daily operations or activities at the exercise target sites, and that no laws will be broken. It addresses any and all safety issues that may arise.

Exercise time-out. This section details the circumstances and the means by which a Red Team participant or SIMCELL controller should declare an "exercise time-out" to present the unique identification to the friendly force when real-world considerations or safety issues are a concern.

Step 3: Synch with MSEL

When Physical Red Teaming is conducted in conjunction with an information/intelligence-based prevention exercise, Red Team actions and the expected resulting player actions need to be reflected in the MSEL. The MSEL drives exercise play by controlling the release of information/intelligence-based injects. It is complemented by the actions of Red Team operators when those actions are detected by players.

The UA group being portrayed by the Physical Red Team is simultaneously exposed to players through MSEL injects. Information and intelligence fusion, analysis, and sharing activities will be generated by injects fed through the participating Federal and local networks and by real-time responses to Physical Red Team activities occurring in the field. The scenario unfolds over a pre-determined notional timeline, and Red Team activities reflect the adversary's planning, preparation, and execution phases. The timing of these activities should be consistent with the intelligence injects on the notional exercise timeline to provide a realistic union of MSEL-driven injects with on-the-ground activity. Synchronizing the Red Team activities with the MSEL will allow exercise players to develop the threat picture and react to the indications and warnings thus ensuring a coherent and consistent exercise.

The Operations Chief is responsible for sequencing Red Team activities within the MSEL, in order to keep Red Team operators fire-walled from expected player actions and other detrimental information. Red Team activities should be synchronized with the MSEL no later than the third planning conference and reviewed at the FPC.

Step 4: Select and Train Red Team Operators

Before the Red Team can be assembled, the Red Team Operations Leader must be designated. Selection of the Red Team Operations Leader should be discussed at the Concepts and Objectives Meeting and should take place as soon as possible. The selection itself is made by the exercise planning team and should be based on the individual's knowledge, skills, and abilities to safely and effectively plan and carry out Physical Red Team operations. This individual should be an experienced leader and skilled operations planner, and he/she should have a detailed understanding of the scenario and the selected UA model.

Selection. Individual Red Team operators should be selected based on their knowledge, skills, and abilities to accurately portray the UA characters they are assigned. The Red Team Operations Leader will work with the exercise planning team to identify Red Team operators who are able to perform the following tasks:

- React to exercise events with maturity and adhere to safety requirements
- Physically conduct proposed operations
- Study and portray a specific terrorist and the group to which they belong
- Appropriately reflect the given terrorists' knowledge, skills, and abilities
- Realistically represent the terrorists' background, culture, and behavior
- Participate in operations planning and reporting

Red Team operators should be identified as soon as work has begun to define Physical Red Team activities. Operators should be selected from participating jurisdictions that can provide the significant time commitment to support the development and execution of Physical Red Team activities.

Once selected, Red Team operators should begin preparing for their roles as soon as possible. Preparation must take place before operators can begin to take part in any of the Red Team Operational Planning Process. The Red Team Operations Leader guides this preparation, during which Red Team operators must immerse themselves in the roles which they are intended to play, undergoing a process similar to the Analytical Red Teaming that is employed in discussion-based exercises. Operators must also be familiar with any and all CONOPS already developed and remain aware of any changes made to them during exercise play.

Role Immersion. All Physical Red Team members should strive to truly know the enemy which they portray. Red Team members must study the selected UA, memorize aspects of their characters' dossiers, and familiarize themselves with the targets and areas of operation. Each Red Team operator should receive an overall UA group profile, which outlines the ideology, motivation, and background developed for the local cells or networks. The UA group profiles are provided to Red Team members by the exercise planning team. The profiles will contain general information, which may include the following:

- Group composition
- Political, religious, or ideological aims
- Objectives
- Motivations
- Command-and-control structures
- Operational organizations and external ties
- Internal and external support structures
- Headquarters, areas of operations
- Fronts and alliances
- State and government ties
- Training

- Tactics and operations
- Attack methodology
- Key operational considerations
- Decision-operation cycle
- Logistics
- Financing
- Ties to criminal activities
- Weapons and ammunition
- Combat effectiveness
- Key personnel
- Culture
- Threats to U.S. Homeland

Red Team operators must know and understand the background information on the particular local cell(s) or network(s) for the exercise. Clear understanding of the cell(s) and/or network(s) will allow them to create a larger, more robust picture of the adversary and the connections between the characters they portray. Furthermore, operators can maintain their characters superiorly with greater knowledge of the cell, network, and character background.

During preparation, Red Team operators should be enlisted by the Red Team Operations Leader to help plan the OPORDs in a manner consistent with the portrayal of their characters. Red Team members should be oriented to the following:

- Adversary's ideology – the driving belief(s) of the UA group in the exercise
- Adversary's motivation – the reason(s) for attack
- Adversary's capability and intent – the skills and abilities of the UA group to conduct the exercise operations and attack, and the desired outcome(s)

Red Team operators will receive their UA characters' dossiers and the dossiers of the other cell members. Learning the dossiers will help Red Team members interact with each other, appropriately and realistically fulfill their role in the cell, and better participate in the exercise.

The dossiers contain baseline information on the individual that is in reflected in the scenario and consistent with the UA group profiles, such as:

- Name
- Aliases
- Date of birth[*]
- Place of birth

[*] These characteristic should be specific to the Red Team operator portraying the individual character.

- Nationality
- Height*
- Weight*
- Build*
- Hair*
- Eyes*
- Complexion*
- Sex*
- Occupation
- Formal education
- Military training
- Other
- Known associates
- Known travel
- Background

The information contained in the dossier can be augmented to support exercise objectives so long as the additions or changes do not change the scenario and are consistent with the UA group profiles. For example, once the Red Team operator is selected, his or her photograph should be added to the dossier, so that it may be used in information-based exercise injects.

Review of Plans and Procedures. Physical Red Team members must be intimately familiar with the given CONOPS and the process of planning an operation. Such elements include:

- Reasons for choosing the particular targets and physical information about them;
- The UA's ultimate goal for the attack;
- Sources of useful information that the terrorists would be able to access; and
- ALL SAFETY GUIDANCE CONCERNING THE EXERCISE, specifically the ROEP.

Step 5: Develop and Approve Red Team Operational Order (OPORD)

The Operational Order (OPORD) provides the confirmed details of a Physical Red Team activity. This document serves as the basis of discussion for the Red Team Mission Briefing, held among operators and safety controllers prior to each operation. It also serves as the actual operator instructions for the conduct of the given activity. OPORDs are developed, as much as possible, in a manner that would be consistent with the operational planning of the terrorist group being portrayed.

TIP: Assign a chronologically sequential number to each OPORDs to facilitate communication regarding each operation.

The necessary components common to all Physical Red Team activities are also common to all OPORDs. They include:

- **Individual operational roles.** Each operator will perform a specific role in the cell. Basic roles include the following:
    - Command and control
    - Logistics
    - Communications
    - Security
    - Tactics/execution
    - Specialized expertise, such as chemical, biological, nuclear, or explosives expertise

  The Red Team Operations Leader will identify the operational roles for each Red Team member.

- **Individual logistics responsibilities.** Red Team members will be responsible for various logistical assignments, both in preparation for exercise play and during exercise play. During planning, operators may be responsible for obtaining video and/or sound recording devices, vehicles, or communications equipment. During the operation, Red Team members may be responsible for driving, monitoring, or coordination.

- **Safety issues.** Any/all specific safety issues that apply to a given operation should be included in the corresponding OPORD. Red Team operators should further review the OPORDs to identify potential additional safety issues. Safety is paramount, and Red Team participants must be aware of potential safety concerns and unsafe conditions. Any exercise participant can declare an exercise time-out based on a safety issue during Red Team operations. To address this potentiality, the loss of communications, or the occurrence of real-world events, a plan of action should be developed to address an exercise time-out.

- **Detailed timeline.** The expected/approximated times at which significant events will occur should be included in the OPORD. Examples of significant events include, but are not limited to departure from the "terrorist safehouse," communications check, entry into a given perimeter, approaching a Blue Team member, departing from a target site, or reporting to the SIMCELL.

TIP: Format timeline to leave space to record the actual times at which significant events occur.

The OPORD is prepared by the Red Team Operations Leader and Red Team operators, and should be reviewed at the FPC and finalized and submitted to Red Team operators, safety controllers, and evaluators no later than 48 hours prior to an operation. *See HSEEP Volume IV for a sample Red Team Operational Order (OPORD).*

Step 6: Conduct Red Team Operations

All Red Team operations conducted in support of prevention exercises must be consistent with the overall exercise scenario and coordinated with SIMCELL controllers to ensure that they reflect the terrorist actions described by exercise intelligence and law enforcement injects. It is extremely beneficial for the designated Red Team Liaison to remain in the physical SIMCELL location during Red Team operations. SAFETY IS THE MOST IMPORTANT

CONSIDERATION DURING THE CONDUCT OF RED TEAM OPERATIONS. The following section describes the events and activities that must occur prior to, during, and immediately following the execution of every Physical Red Team operation.

48-Hour Notification. The distribution of OPORDs will be the final notification of Red Team activity 48 hours prior to its execution. The Red Team Liaison is responsible for distributing approved OPORDs to appropriate members of the exercise planning team within this timeframe.

A Red Team Mission Briefing may be conducted by the Red Team Operations Leader in conjunction with this notification. This briefing to the exercise planning team provides a mission overview and specific information for the impending event. The Red Team Operations Leader should not be present for other exercise-specific discussions held by the exercise planning team, to reinforce the firewall. The Red Team Operations Leader can discuss the following issues in the Red Team Mission Briefing:

- The mission and each event that will be conducted;
- Safety and security factors that might affect this activity;
- Real-world developments that might affect or be affected by this activity; and
- Final approval from the exercise director.

Pre-Operations Briefing. On the day of a Red Team operation, Red Team operators, safety controllers, and evaluators will gather in a convenient location away from the operational area to conduct final safety, equipment, timing, and communications checks. They should discuss any specifics of the Mission Briefing; review proposed actions; and ensure that activities, roles, responsibilities, and operational procedures are outlined and understood. These participants will then deploy to an area near the operation site after the Pre-Operations Briefing for a communications check with the SIMCELL.

Communications Check with SIMCELL. This communications check ensures that an additional layer of safety is in place for the conduct of a Physical Red Team operation. Red Team safety controllers should contact and receive acknowledgement from the safety officer and senior controller in the SIMCELL prior to the commencement of each Red Team activity. The following steps must be taken to gain authorization to begin Red Team activity:

- The senior Red Team operator will notify the Red Team Liaison – in the SIMCELL – that the Red Team is in position and ready.
- Red Team safety controllers will notify the lead safety officer that they are in position and ready.
- Red Team evaluators will notify the senior SIMCELL controller that they are in position and ready.
- Upon notification that each team is in position and ready, the senior SIMCELL controller determines whether to begin the operation. The senior controller should then issue a “GO” authorization to the lead safety officer and Red Team Liaison. These individuals will notify the safety controller and senior Red Team operator, respectively.
- The senior Red Team controller allows Red Team activity to begin, following the established ROEP.
- Red Team deploys to target site.

Conduct Operation. Once authorization is received and communications are confirmed, the Red Team deploys to the target site and conducts its activities according to the OPORD. Red Team operators should apply their knowledge of terrorists' motivations, organization, targeting, tactics, techniques, procedures, and equipment and behave accordingly.

Players will not have prior knowledge of the specific Red Team operations and should treat the actions and behaviors they observe as real. Players will use routine, in-place communications systems. Additional communication assets may be made available as the exercise progresses. (Note: the need to remain capable of responding to a real-world incident may preclude the use of all communications channels or systems that would usually be available.)

If a safety or security issue emerges, any Red Team operator, safety controller, or evaluator, as well as any SIMCELL controller, can call an exercise time-out and immediately stop play. Play can resume or be suspended as necessary.

Communications Check with SIMCELL. Upon conclusion of each event, safety controllers should notify the lead safety officer. The safety officer then notifies the senior SIMCELL controller that the given Red Team operation has safely concluded.

Hotwash. Upon completion of each activity, Red Team operators, safety controllers, and evaluators should gather at a convenient location away from the operational area and hold an informal debriefing on the day's activities. This hotwash is an opportunity for important evaluative and procedural (i.e., safety-related) issues to be recorded while they are fresh in the participants' minds. The Red Team Operations Leader should lead the hotwash and try to capture information on the following topics:

- Safety and security issues;
- Real-world issues;
- Mission results: the extent of the Red Team's ability to accomplish its mission in each of the events;
- The effects that the mission results might have on the planning and/or execution of future Red Team activities; and
- Specific questions and answers, as necessary for further development of injects.

Step 7: Report on Operations and Provide AAR Input

All Red Team operations and activities should be documented so that they may be analyzed and used when developing the exercise AAR. As they conduct activities and interact with exercise players, Red Team operators serve as both scenario elements and evaluators.

For each activity Physical Red Team participants should combine observations and limited analysis into a written post-operational report. The exercise planning team operations chief should designate a Red Team leader, operator, safety controller, or evaluator to be ultimately responsible for each post-operational report. The responsible participant should be sure to collect observations and analysis from the remainder of the group.

Each post-operational report outlines a given Red Team activity. It serves a dual purpose of providing the exercise planning team/SIMCELL with instant feedback needed to alter future injects as necessary; and contributing firsthand observation and analysis to the evaluation team for inclusion in the final AAR.

Red Team post-operational reports contain certain details of the Red Team activities, as measured against the planned operation outlined in the OPORD. The reports should include information relevant to the exercise objectives and relative to the expectations presented in the OPORD, as well as the following:

- Actual time(s) of significant events
- An account of all actions taken by Red Team operators, safety controllers, and evaluators during the operation
- Significant occurrences
- A narrative of the operation
- Comments from the operators on the perceived success/failure of the mission
- Effects of the mission on planning and execution of future actions
- Red Team operators' real names, character names, and contact information
- Logistics information
- A list of all communications equipment used
- A list of visual or sound recording devices used
- Vehicle make, model, and license plate information
- All other supporting equipment and documentation, including but not limited to fraudulent documentation, storage facilities, rental equipment, etc.