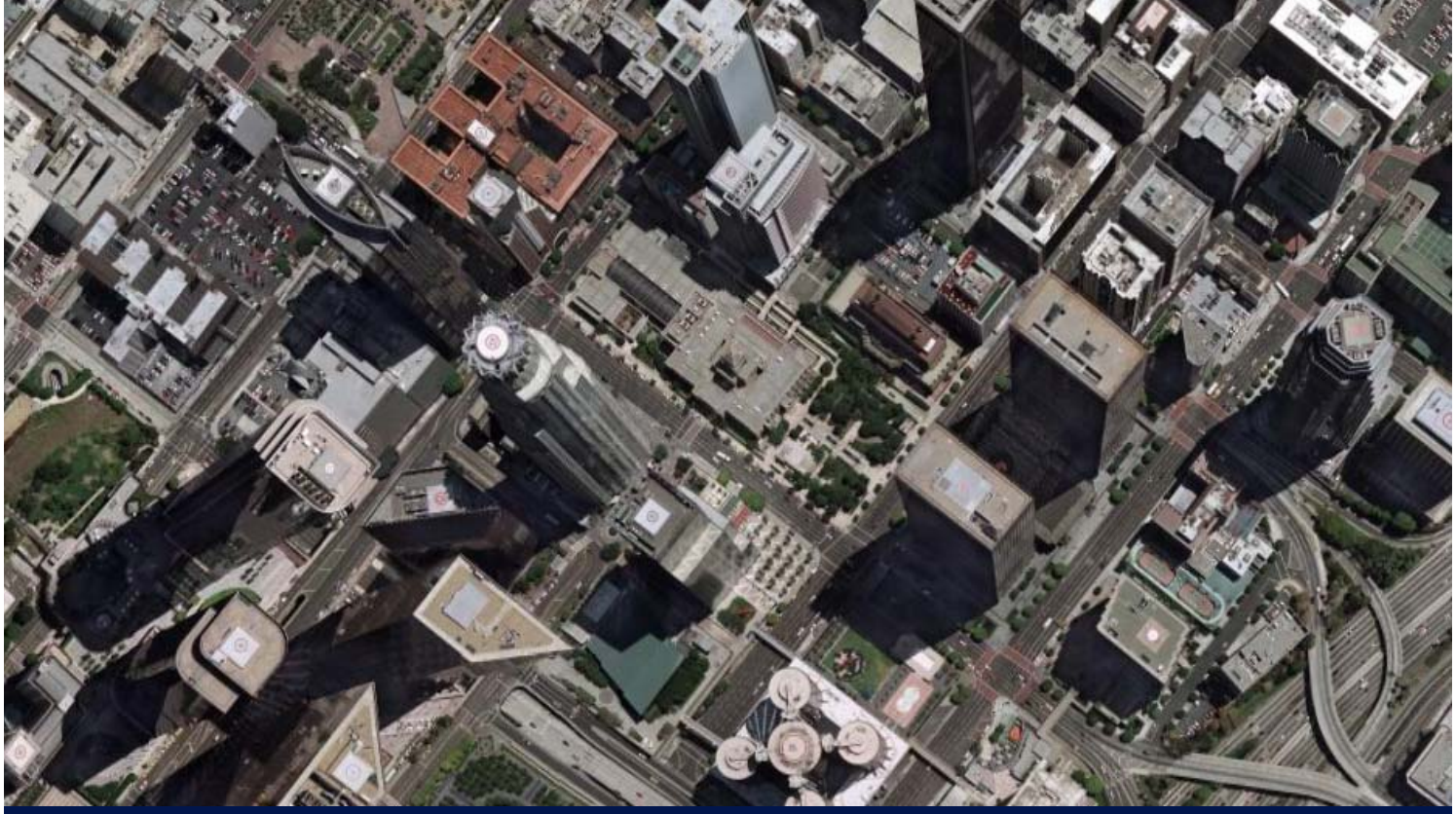

Multi-Jurisdiction IED Security Plan

Planning Guide

Homeland Security

THIS PAGE IS INTENTIONALLY BLANK

Table of Contents

Executive Summary 2
1.0 Introduction 3
1.1 Purpose 4
1.2 IED Threats 5
2.0 Multi-Jurisdiction IED Security Plan Development Process 7
Step 1: Identify Planning Area 8
Step 2: Identify Facilities or Locations of Concern 14
Step 3: Identify Security Partners 14
Step 4: Identify Site-Specific Considerations 16
Step 5: Identify IED Security Needs 19
Step 6: Assess Current Capabilities and Assets 20
Step 7: Identify Steady-State Actions 22
Step 8: Identify Threat-Initiated Actions 25
Step 9: Validate Plan 29
Step 10: Establish Plan Maintenance Process 31
Appendix A –Multi-Jurisdiction IED Security Plan Checklist 33

Table of Figures

Figure 1: IED security timeline 3
Figure 2: Sample IED types 5
Figure 3: Selected IED incidents 1998-2006 6
Figure 4: Multi-Jurisdiction IED security development process 7
Figure 5: Los Angeles 8
Figure 6: CIKR Sectrors 10
Figure 7: NIPPRisk Management Framework 11
Figure 8: Los Angeles with identified CIKR and soft targets 12
Figure 9: Key security partners 14
Figure 10: Additional IED TTP references 17
Figure 11: IED-security related TCL capabilities 19
Figure 12: NCAD screenshot 21
Figure 13: Example steady-state actions 23
Figure 14: Example threat-Initiated Actions 26

Executive Summary

The Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP) Planning Guide assists multi-jurisdiction areas in developing a detailed IED security plan. The IED security plan outlines specific bombing prevention actions that reduce vulnerability and mitigate risk against the primary terrorist IED attack method within a multi-jurisdiction area.

The IED Threat

Improvised Explosive Devices (IEDs) are a preferred method of attack for terrorists around the world. IEDs are relatively simple to assemble and employ, and provide terrorists with an operational flexibility that poses great challenges for those responsible with preventing their use or mitigating their effects. Furthermore, the tactics that terrorists use to employ IEDs are continually evolving. Suicide bombers, vehicle-borne devices, simultaneous and coordinated attacks, and the targeting of emergency responders with secondary devices are a few of the creative methods terrorists use to increase the disruption and fear caused by IEDs.

IED Security

"IED security" is defined as the condition wherein the risk posed by IED attacks is managed to the greatest extent possible. Achieving IED security within a multi-jurisdiction area requires a properly balanced approach that encompasses the efforts of all those working to apply law enforcement, protective measures, and emergency response resources, across the continuum of homeland security missions—prevention, protection, response, and recovery. While acknowledging the importance of each mission area, this guide emphasizes the development of actions multi-jurisdictions should take during the prevention and protection stages of IED security.

MJIEDSP Development

The development of a MJIEDSP is a cooperative effort requiring the collaboration of numerous agencies across multiple localities, disciplines, and levels of government. The development methodology includes a 10-step process to be completed jointly through the accompanying MJIEDSP template. As planning partners read through this guide, outputs are identified for each step, which the planner will then complete by filling out specific sections within the template. Together, both documents guide the planner in determining key threats and vulnerabilities, and finally in developing a plan that identifies specific *steady-state* and *threat-initiated* actions to reduce the risk of an IED attack to their primary area of operations. Both the initial plan and security partnerships can and should be expanded using this repeatable process to further define and improve IED security actions within the planning area.

> The Multi-Jurisdiction IED-Security Plan development process provides a consistent and repeatable process to execute steady-state and threat-initiated IED prevention and response actions.

Conclusion

This guidance is intended to support State, local, and tribal efforts to enhance their IED security capabilities by adopting effective practices to maximize available resources to prevent and respond to an IED threat. The MJIEDSP that results from this process should both determine what actions are necessary to enhance IED prevention and protection capabilities of multi-jurisdiction area, and, ultimately, be used by operational decision-makers to determine what steps to take during an IED incident.

1.0 Introduction

Acknowledging the need to effectively prevent and protect against an IED attack is the first step in overcoming the challenges of achieving IED security. Homeland Security Presidential Directive 19 (HSPD-19) has called for a national approach for achieving IED security that relies on common goals, measurable objectives, and dedicated partnerships among security partners such as private citizens, private sector organizations, and relevant agencies at all levels of government.

> The term "IED security" represents the condition wherein the risk posed by IED attacks is managed to the greatest extent possible. Risk, as defined by the National Infrastructure Protection Plan (NIPP) is defined as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event.

This document, the *Multi-Jurisdiction IED Security Planning Guide*, complements the strategic framework of the HSPD-19. Just as the HSPD-19 sets forth goals and a framework for integrating and coordinating national IED security efforts, this guide provides a repeatable process to facilitate the integration and coordination of IED security prevention and protection efforts within a locally defined area. To this end, this process satisfies the objective to "develop regional bombing prevention plans" which is defined within the HSPD-19 as a priority for the Nation, and supports State and local jurisdictions in developing a standardized plan to prevent an IED attack, identified herein as a Multi-Jurisdiction IED Security Plan (MJIEDSP).[1]

The chart below outlines common phases of terrorist IED plots and describes, in general terms, the periods in which the key elements of the homeland security mission spectrum overlap with opportunities to intervene. In a MJIEDSP, actions taken by security partners should primarily address the prevention of and protection against an IED attack within the given planning area.

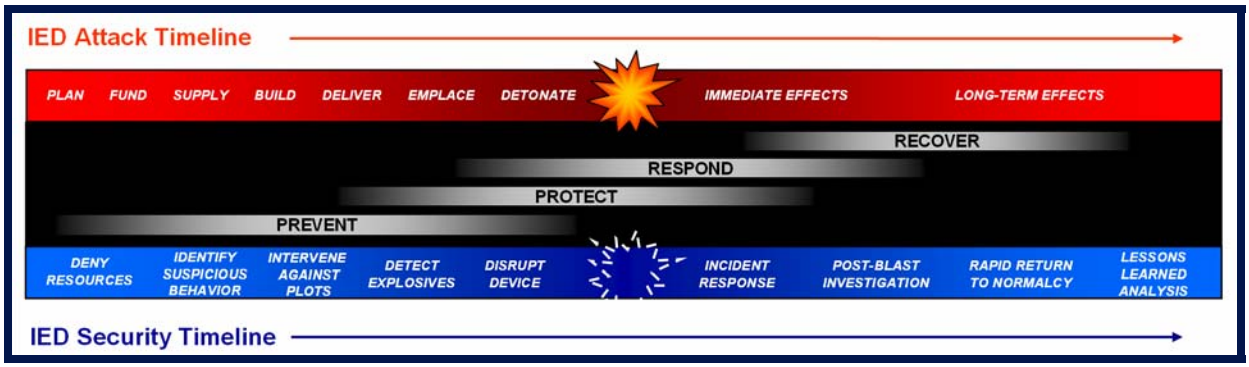

Figure 1: IED security timeline

[1] Note: While the primary goal of a MJIEDSP is to prevent an IED attack, emergency services should consider secondary devices when responding to an incident. Moreover, during the recovery stage, post-blast investigation is critical to collecting evidence and reducing the risk of a subsequent attack by providing investigators with intelligence for use in preventing future attacks and potentially capturing the perpetrators.

1.1 Purpose

The purpose of the *Multi-jurisdiction IED Security Planning Guide* is to provide an organized and repeatable method to:

- Determine key geographical and jurisdictional boundaries as a "planning area";
- Identify security partners and available resources within the planning area;
- Describe specific steady-state and threat-initiated actions that may be required by multiple Federal, State, or local agencies to address IED threats, and must be prepared for; and
- Assist in the identification of shortfalls in multi-jurisdiction bombing prevention capabilities which may then be used in applying for Federal homeland security grants.

The environments which multi-jurisdictions must prepare for are defined as follows:

A **steady-state** environment is defined as a "normal" situation in which no specific threats have been articulated for a particular region, sector, or location. Responsible emergency management and law enforcement entities within the jurisdictions that make up a planning area will not take special or extraordinary action during this environment. Steady-state tasks or actions may include routine security procedures or general preventive and protective measures to deter surveillance and attack planning or devalue a potential target.

A **threat-initiated** environment is defined as a situation in which a threat has been made to the region, a critical infrastructure sector such as a transportation system, or a specific facility. Threat-initiated actions are enacted by security partners with the purpose of preventing and protecting against a specific attack. Both the deployment of canine explosives detection to situations in which a specific hazard has not yet been identified, and the notification of bomb squads to disrupt or render safe an actual or suspected device are examples of different threat-initiated actions.

For each situation, jurisdictions should both train responders in IED prevention and protective actions, and inform the general public on what to do during each type of threat environment. The correct categorization of situations and the accurate identification of threats are essential to consistently and correctly execute IED security actions.

This guidance is intended to support State, local, and tribal government efforts to enhance their IED-security capabilities as they adopt effective IED security practices and maximize available resources to prevent and protect against an IED threat. The MJIEDSP that results from this process is not meant to outline standard operating procedures; but rather, should both identify what actions are necessary to enhance IED prevention and protection capabilities of multi-jurisdiction areas, and, ultimately, be used by operational decision-makers to determine what general steps to take during an IED incident.

1.2 IED Threats

IEDs are technically defined as "…devices placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals, designed to destroy, disfigure, distract or harass. They may incorporate military stores, but are normally devised from non-military components."[2] More generally speaking, IEDs are bombs constructed from readily available materials, which may include conventional or homemade explosives. While the term "conventional explosives" generally refers to commercial products or military ordnance, IEDs can include explosive materials or other components scavenged from such sources, or they may be fashioned using legitimate consumer products and materials intended for innocuous use, such as propane, diesel fuel, and fertilizer.

The construction and deployment of an IED is not standardized. These devices can be produced in varying sizes, functioning methods, sophistication, complexity, containers, and methods of delivery (Figure 2). The types and quantities of IEDs used are generally related to the target for which they are intended, and can be built for use as a single device, as multiple devices detonated independently, or detonated in a chain reaction.

Significant large-scale international IED attacks that have killed hundreds of civilians help inform our understanding of threats that could occur domestically in the future (Figure 3). These explosions varied in size, type, number, and location, and were executed by a variety of perpetrators with different motivations.

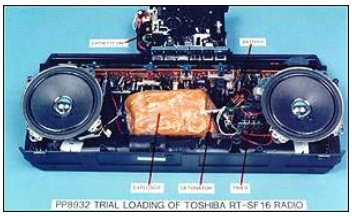 Mockup of IED concealed in consumer electronic device used to destroy Pan-Am flight 103 over Lockerbie, Scotland	Suicide vest used by LTTE (Tamil Tigers) in Sri Lanka	Vehicle-Borne IED (VBIED) used in Iraq and Afghanistan
Diagram of device used by Richard Reid (HMS via *TRIPwire*)	Unexploded backpack IED used in the March 11, 2004 Madrid bombings	Unexploded peroxide-based IED with shrapnel load used in the July 7, 2005 London bombings

Figure 2: Sample IED types

[2] Director for Operational Plans and Joint Force Development, Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* April 12, 2001. As amended through November 9, 2006. Washington, DC: United States Department of Defense.

Similar IED attacks have also occurred within the United States. Most notable are the first attack on the World Trade Center in 1993 in New York, NY; the Alfred P. Murrah Federal Building in 1995 in Oklahoma City, OK; Centennial Park Olympic bombing in 1996 in Atlanta, GA; and the string of letter bombs used by the Unabomber from 1978-1995.

Selected IED Incidents 1998-2006		
Event	**Year**	**Casualties**
Mumbai, India – train bombings	2006	207
London, England –train and bus bombings	2005	56
Madrid, Spain – train bombings	2004	191
Bogotá, Colombia – social club bombing	2003	36
Kuta, Bali – nightclub bombing	2002	202
Port of Aden, Yemen – USS Cole, water-borne VBIED	2000	17
Khobar, Saudi Arabia – VBIED	1998	20

Figure 3: Selected IED incidents 1998-2006

Historically, IEDs are detonated in single explosive device events. However, recent trends in Iraq and Afghanistan, in addition to specific incidents, such as the 2002 Bali nightclub bombings point to detonations occurring simultaneously or consecutively in multiple locations. For some of these multiple-device events, secondary devices were detonated to target the emergency workers responding to the initial blast.

2.0 Multi-Jurisdiction IED Security Plan Development Process

The MJIEDSP development process builds upon the capabilities-based planning approach outlined in the National Preparedness Guidelines. Using a common framework and a repeatable process, this methodology assists the planner in both identifying IED prevention and protection capabilities and coordinating and prioritizing security actions that must be executed across multiple jurisdictions during periods of heightened threat levels or in response to an actual IED incident.

The 10 steps of the MJIEDSP development process provide the structure for the planning process. Planning actions are identified within each step along with outputs, outcomes, and metrics to track progress toward improved IED security within the planning area. The accompanying MJIEDSP plan template is provided to capture important information for use in developing a finalized MJIEDSP. In addition, Appendix A of the guide provides a checklist for the planner to gauge his or her progress as they accomplish each step.

The steps are:

1: Identify the Planning Area
2: Identify Facilities or Locations of Concern
3: Identify Security Partners
4: Identify Site-Specific Considerations
5: Identify IED Security Needs
6: Assess Current Capabilities and Assets
7: Identify Steady-State Actions
8: Identify Threat-Initiated Actions
9: Validate Plan
10: Establish Plan Maintenance Processes

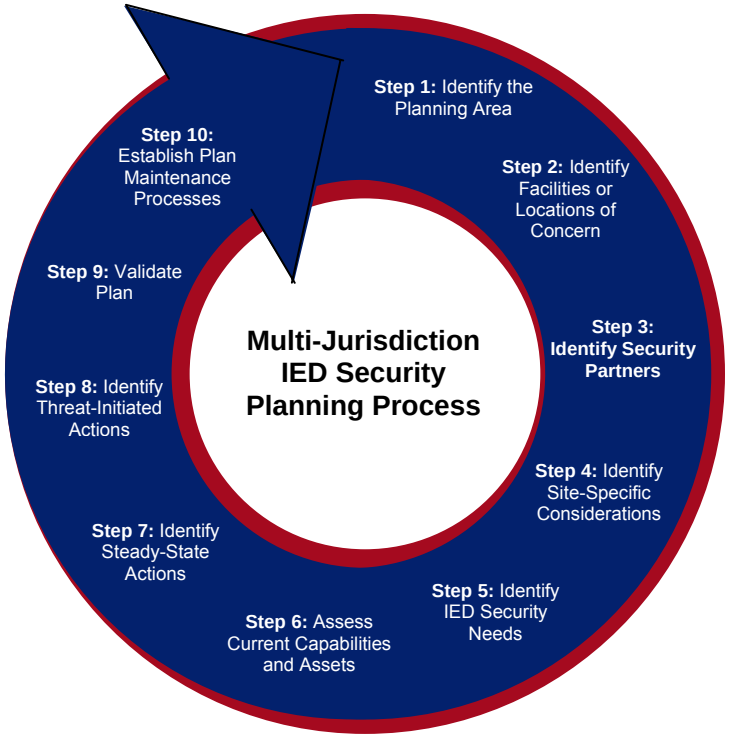

Figure 4: Multi-Jurisdiction IED security development process

Step 1: Identify Planning Area

The first step in developing a MJIEDSP identifies the applicable geographic area and corresponding jurisdictions. A multi-jurisdiction planning area consists of a primary area of operations that may include Federal, State, and local government security partners. Neighboring jurisdictions made up of additional security partners should also be included in the planning area, and may provide assistance if the primary area of operations becomes overwhelmed during an IED event.

Planning Actions:

1.1: Identify the primary area of operations

1.2: Identify neighboring jurisdictions that may provide assistance

Output: A planning area that clearly identifies the boundaries of the primary area of operations

Outcome: A common understanding of the planning area

Metric: Increase in responders, leaders, and managers who understand the area in which they must operate

1.1: Identify the primary area of operations. To determine the primary area of operations, planners should consider the impact of Federal definitions such as Urban Area Security Initiatives (UASI) on defining a region's area of operations. The UASI Program is designed to enhance the ability of first responders and public safety officials to secure the area's critical infrastructure and respond to potential acts of terrorism. Some regions that participate under the UASI program may have already developed a terrorism incident emergency operations plan defining the primary area of operations. Emergency planners should leverage these existing efforts for help in defining the jurisdictions for which they must plan for.

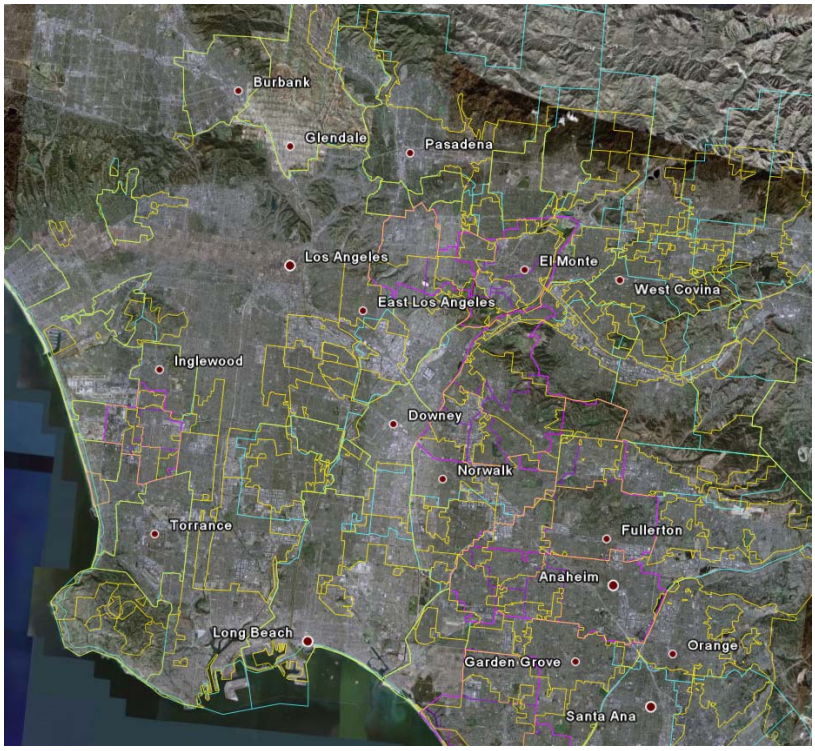

Figure 5: Los Angeles

For example, the UASI area for the area around the city of Los Angeles provides an example

of a potential primary area of operations that includes multiple jurisdictions. It not only includes the city itself, but also surrounding cities within greater LA County, such as Burbank, Pasadena, and Long Beach (Figure 5).

In addition, in many regions, emergency preparedness functions may not fall along the same jurisdictional or political boundaries. For example, law enforcement regions may not be contiguous with emergency medical services regions, which in turn, may not fall under the political jurisdiction of a governing mayor. During this step, planners should ensure that jurisdiction's legal and political boundaries are clearly understood and recorded.

Finally, the completion of this step should also produce Geographic Information System (GIS) mapping products, such as Google Earth images, that visually identify the boundaries of multi-jurisdiction planning area.

1.2: Identify neighboring jurisdictions that may provide assistance. In the event of an incident that overwhelms a primary area of operation's capability to respond, it is important to identify neighboring jurisdictions, including State and Federal entities that should be included in the planning area. These neighboring jurisdictions, identified by the presence of facilities under the authority of such entities as the State police, National Guard units, and the Department of Defense may be able to provide valuable assistance during a heightened IED threat alert. Many of these jurisdictions have capabilities that could be called upon to augment the response within the primary area of operations. For example, nearby National Guard bases may have explosive ordnance disposal (EOD) units that could provide assistance to public safety bomb squads in the field. After identifying these neighboring jurisdictions and potential planning partners, the planner should consider developing memoranda of understanding (MOUs) and mutual aid agreements (MAAs) so that assets from these jurisdictions can provide support if needed. Identifying the security partners within these jurisdictions and developing MOUs are addressed in Steps 3 and 8.

Step 2: Identify Facilities or Locations of Concern

After the planning area and security partners have been determined, planners are now ready to identify facilities or locations within the planning area that may be potential targets for an IED attack. A key factor to consider for initial selection are assets already identified via relevant critical infrastructure protection programs, including the Buffer Zone Plan development process. Partners should refer to Federal, State, or local asset inventories, planning documents and strategies, or use their jurisdiction-specific expertise to assemble an inventory of facilities or locations of concern.

Planning Action:

2.1 Identify Critical Infrastructure and Key Resources (CIKR) assets, systems, and networks within the primary area of operations

2.2 Identify other facilities or locations of concern, such as "soft targets" and other vulnerable sites within the primary area of operations

2.3 Prioritize identified facilities and soft targets according to their criticality

Output: List of prioritized CIKR sites and soft target locations, and GIS images, including a criticality assessment for each facility or soft target

Outcome: Improved inventory and awareness of CIKR sites

Metric: Increase in prioritized CIKR sites and soft targets which have been identified as potential targets for IED attacks

2.1: Identify Critical Infrastructure and Key Resources (CIKR) assets, systems, and networks and their buffer zones within the primary area of operations. Terrorist goals and motivations most likely focus on critical infrastructure and key resources (CIKR) and remain a highly attractive target for attack. CIKR are attractive targets because of the significant and far-reaching physical, economic, and psychological impact of disrupting or disabling a facility or system so important to day-to-day life. A successful attack on a critical infrastructure facility can have dire loss of life consequences. Security partners must therefore identify potential CIKR targets within the planning area based on their vulnerability to attack and the resulting consequences for the surrounding community.

CIKR are divided into 18 sectors pursuant to Homeland Security Presidential Directive/HSPD-7 and the National Infrastructure Protection Plan (NIPP) (Figure 6). The NIPP seeks to enhance "protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by

1. Agriculture, food (meat, poultry, egg products)
2. Public health and healthcare
3. Food (other than meat, poultry, egg products)
4. Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)
5. Banking and finance
6. National monuments and icons
7. Defense industrial base
8. Chemical
9. Commercial facilities
10. Dams
11. Emergency services
12. Commercial nuclear reactors, materials, and waste
13. Information technology
14. Telecommunications
15. Postal and shipping
16. Transportation systems
17. Government facilities
18. Critical Manufacturing

Figure 6: CIKR sectors

terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."

The cornerstone of the NIPP is its risk management framework, which provides a standardized approach to protecting CIKR including *identifying assets, systems, networks, and functions*; assessing risk based on consequences, vulnerabilities and threats; establishing priorities based on risk assessments; implementing protective programs; and measuring effectiveness.

Based on guidance from DHS, and in accordance with this risk-management framework, Sector-Specific Plans (SSPs) are being developed jointly by Federal, State, local, and tribal homeland security partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all sectors, as well as a national framework for each sector that guides the development, implementation, and updating of State and local homeland security strategies and CIKR protection programs. Among other things, SSPs serve to define sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies, as well as identify priority CIKR and functions within the sector. If appropriate, planners should use these SSPs to identify CIKR within their own planning area. If SSPs are not available or not applicable to the planning area, planners should leverage the NIPP risk management framework in alternate ways to identify and prioritize potential CIKR targets.

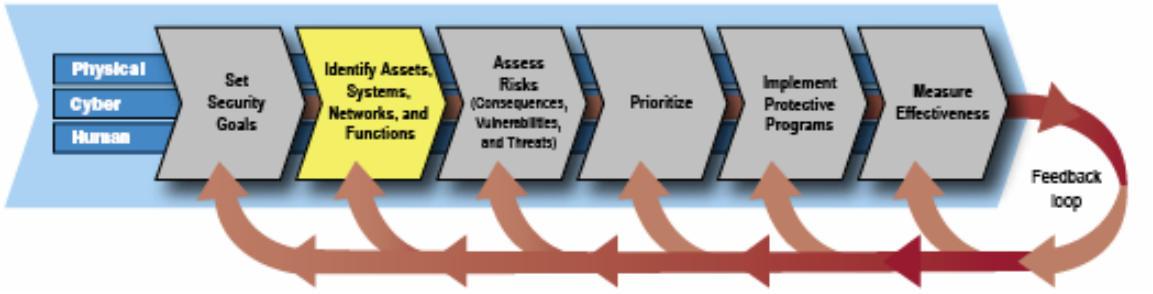

Figure 7: NIPP Risk management framework

States and localities currently use this framework to identify facilities of concern when applying for grants under the Buffer Zone Protection Program (BZPP). Under this grant justification process, security partners have identified the assets, systems, and networks within their planning area that fall within these 18 sectors and prioritized them utilizing the NIPP risk management framework. Emergency planners should either leverage this framework to identify facilities for use in this planning process, or draw from pre-existing efforts.

Planners may also use additional GIS mapping tools such as the Integrated Common Analytical Viewer (ICAV)[3] and the DHS Office for Bombing Prevention (OBP) National Capabilities Analysis Database (NCAD) to locate these facilities within their planning area and map their relative location to other facilities and response assets. ICAV provides various geospatial data layers (imagery, roads, state boundaries, etc) as well

[3] ICAV is located on the Homeland Security Information Network (HSIN). To gain access to HSIN, you can contact the HSIN helpdesk at 703-674-3003 24 hours/day. The website is www.hsin.gov.

as nationwide infrastructure information across all 18 sectors. NCAD serves as an online repository of the location, status, and capabilities of public safety bomb squads, explosives detection canine teams, and dive teams throughout the country. GIS tools such as ICAV and NCAD allow planners to compare the locations of facilities of concern with available response assets within the multi-jurisdiction area.

2.2: Identify other facilities or locations of concern, such as "soft targets" and other vulnerable sites within the primary area of operations. Planners should also identify those geographic areas or "high-risk clusters" of assets which may be potential targets for terrorist IED attack. This category may include "soft targets" such as malls, schools, restaurants, hotels, and other high-traffic public areas. Attacks on soft targets are often perpetrated because of their massive and immediate social and political impact. An attack on a soft target may also have the potential to cause a much greater loss of life than one targeting a hardened CIKR facility. As national critical infrastructure protection efforts continue to harden CIKR, the relative lack of protective measures surrounding malls, restaurants, hotels, and other soft targets potentially makes these locations even more attractive and vulnerable to terrorists. Planners must therefore identify any facilities or locations of concern that may not fall under CIKR, but could be a potential target for a terrorist attack resulting in significant consequences for the surrounding community. Figure 8 shows an aerial photo of Los Angeles with identified CIKR and soft target sites.

Figure 8: Los Angeles with identified CIKR and soft targets

2.3: Prioritize identified facilities and soft targets according to their criticality. Criticality refers to the value of the facility and soft target (i.e. the consequences of its damage). This is the primary consideration when determining the priority of a potential target. A facility, location, or soft target is critical when its destruction or damage results in casualties or has a significant impact on the community's political, social, and economic operations.

The criticality of a facility or location must be considered in relation to other elements within the NIPP-identified sector and the effect of its damage to other CIKR sectors or levels of government. Additionally, the value of a target may change as the threat environment evolves or if an IED incident occurs. For example, if a sustained terrorist IED campaign targets all but one water treatment plant in a given area, the remaining plant has a much higher value than before the initial attack. Criticality depends on several factors that include:

- Proximity to local population centers
- Production of critical resources
- Impact on local economy
- Environmental consequences
- Impact on local or regional Security
- Symbolic importance
- Other socio-political impacts

In addition, planners should consider a site's interdependencies with other sectors, including the energy, transportation, telecommunication, and water sectors for example. Lastly, the facilities' lost operation costs, facility replacement costs ,and population impacts must be considered as well. Many facilities have already conducted these assessments, but the planning area may consider conducting a criticality assessment on soft-targets as well. Based on the criticality assessments, planners should then prioritize identified CIKR and soft-targets to protect those facilities that would have the most affect on society if attacked.

Step 3: Identify Security Partners

Once the planning area has been identified, planners can then identify those Federal, State, local, and public and private sector security partners that will be essential in preventing and responding to and IED attack.

Planning Action:

3.1 Identify potential security partners for both your primary area of operations and neighboring jurisdictions determined during Step 1

3.2 Determine the individuals from each agency or discipline that should participate in the planning process

Output: Master Stakeholder Listing

Outcome: All security partners within the primary area of operations and surrounding jurisdictions have been identified

Metric: Increase in number of relevant participants in planning process

3.1*: *Identify potential security partners for both your primary area of operations and surrounding jurisdictions determined during Step 1. For a plan to be effective, it must include all security partners, including Federal, State, and local emergency management, law enforcement, first responders, and selected private sector and public partners that can support efforts to prevent and protect against an IED incident.

The focus of this step should be identifying the security partners within the primary area of operations that would be the first to respond to an IED threat. Collaborating with each entity during the planning process ensures the scope of services provided and the responsibility for each authority are well understood. The National Response Framework's Emergency Support Functions and its Terrorism Incident Law Enforcement and Investigation Annex should be used to identify potential Federal security partners. The following table identifies some of the entities that can provide key services during an IED incident.

Potential Key Security Partners for Multi-Jurisdiction IED Security Planning		
▪ CIKR Owner and Operators ▪ Citizen Corps ▪ DHS Protective Security Advisors ▪ FBI Special Agent Bomb Technicians ▪ Federal Emergency Management Agency ▪ Fire Departments ▪ Fusion/Terrorism Early Warning Centers	▪ Joint Terrorism Task Forces ▪ National Guard/DoD Explosive Ordnance Disposal Units ▪ National Infrastructure Coordination Center ▪ Public/Private Sector ▪ Public Safety Bomb Squads ▪ Public Safety Dive Teams ▪ Sheriff Departments	▪ Special Weapons and Tactics Teams ▪ State/Local Emergency Management ▪ State/Local Law Enforcement ▪ Transportation Security Administration Explosive Detection Canine Teams ▪ Transportation Security Administration Bomb Appraisal Officers

Figure 9: Key security partners

3.2: Determine the individuals from each agency that should participate in the planning process. Once the specific security partners have been identified, leaders and decision makers within each entity should be identified to assist in the planning process. Preferably, those with previous planning experience and extensive knowledge of their mission area and geographic area of operations should be chosen. The capabilities that each entity can provide will be included later in the planning process during Step 7.

Step 4: Identify Site-Specific Considerations

Once the facilities and locations of concern have been identified and prioritized in terms of criticality in step three, the next step is to determine the various vulnerabilities. Vulnerability assessments are common planning tools for homeland security plans. Whenever possible, previously conducted assessments should be used to conduct this planning step.

As specific vulnerabilities are identified, emergency planners can determine the protective measures needed to reduce the risk to a potential target by a successful IED attack. While the previous and following steps may have already been conducted during prior vulnerability assessments or when developing a Buffer Zone Plan (BZP), this information is important for identifying when and how emergency management and law enforcement will address threats that may involve specific sites, multiple sites, and/or BZPs.

Planning Actions:

4.1 Identify viable and likely IED tactics, techniques, and procedures that could be used to threaten the facility or soft target

4.2 Conduct a vulnerabilities analysis of each prioritized CIKR and soft target

Output: Vulnerability assessments for each identified facility or soft target, including a targets and tactic list of possible methods of attack

Outcome: An understanding of the vulnerabilities of prioritized targets within the planning area

Metric: Increase in prioritized CIKR sites which have conducted vulnerability assessments against specific methods of IED attacks

4.1: Identify viable and likely IED tactics, techniques, and procedures that could be used to threaten the facility or soft target. Based on an assessment and analysis of current IED trends and historical consideration of the evolution of IED-related techniques, tactics, and procedures (TTPs), the following are examples of key types of an IED attack:

- Vehicle-borne IEDs (VBIEDs), such as those used in the 1993 World Trade Center and 1995 Oklahoma City bombings, including waterborne IED (WBIED) attacks similar to the *USS Cole* incident;
- Suicide tactics, including those carried out using VBIEDs or focusing on transportation systems such as trains and buses, as demonstrated in the July 7, 2005, London transit bombings;
- Multiple, simultaneous attacks in a single city or region, such as the London, Madrid, and Mumbai attacks;
- Remote-controlled IED (RCIED) methods used daily in Iraq and Afghanistan;

- Secondary devices that are placed at the scene of an ongoing emergency response with the intention of causing casualties among responders or other nearby individuals such as the attack on Bali nightclubs in 2002; and
- Soft target/high-risk re-capture hostile sites or hostage situations in which IEDs present an additional response obstacle such as the Beslan and Columbine incidents.

Emergency planners should use these types of IED attacks to inform their determination of specific vulnerabilities for each facility or locations of concern. After a prioritization of key facilities has been conducted, key threats and tactics can be determined for each facility, and will assist the planner in filling out the accompanying tables in the template. For a more thorough description of IED-related TTPs, planners may consult the additional references described below.

Additional IED TTP references	
Tool	***Application***
Technical Resource for Incident Prevention (TRIPwire)	TRIPwire is an online, information-sharing network for bomb technicians and other law enforcement officials to learn about current terrorist bombing tactics, techniques, and procedures, including IED design and emplacement. By integrating information gathered directly from terrorist groups with analysis and collaboration tools, TRIPwire helps operators anticipate potential threats specific to bombing incidents. Specific information available includes terrorist manuals and videos describing IED manufacture and use, reports on IED incidents, and DHS threat bulletins. Available at (www.tripwire-dhs.net).
National Planning Scenario 8: Chemical Attack – Chlorine Tank Explosion and National Planning Scenario 12: Explosives Attack – Bombing Using Improvised Explosive Devices	Scenarios 8 and 12 addressing both a Chlorine Tank Explosion and a multiple IED attack provide the reader with both the potential steps it takes a terrorist to plan and carryout IED attack, and its subsequent consequences. These scenarios are available upon registration at the Lessons Learned Information Sharing Network (*LLIS.gov*).
Terrorism Knowledge Database (TKB)	A comprehensive and interactive Web-based national information repository on terrorist entities, terrorist incidents, and legal data on terrorism indictments in the U.S. Available at (www.TKB.org).

Figure 10: Additional IED TTP references

4.2: Conduct a vulnerability analysis of each prioritized CIKR and soft target. In most cases, BZPs and vulnerability assessment information will exist describing the security state of sites and locations of concern within the primary area of operations. In the event that vulnerability information is unavailable for some sites, additional security reviews should include an assessment of the facilities' vulnerability to surveillance; physical security such as doors, windows, locks, lighting, fencing, and alarms; nearby bomb disposal and protective force support; and finally a facilities' hiring and other human resource practices.

Several methodologies for assessing site vulnerabilities are currently used throughout the Nation and can be leveraged within the planning area. For example, DHS maintains a BZPP that supports BZP development for selected sites. Additionally, the National

Domestic Preparedness Coalition designed the Homeland Security Comprehensive Assessment Model, (HLS-CAM)[4] which also may be useful in the development of an MJIEDSP. FEMA has also developed a rapid assessment methodology for assessing the vulnerability of buildings to terrorist attacks. When choosing any assessment, planners should consider methods that have already been applied to assets in the area to ensure consistency in planning processes within the area and among the planning partners. Results of vulnerability assessments are important in determining the security needs to reduce its overall risk to an IED attack.

[4] For more information on HLSCAM, please go to http://www.ndpci.us/hls_cam.html.

Step 5: Identify IED Security Needs

Collectively, the planning area must possess a specialized group of capabilities that are specific to IED threats and incidents. Understanding the range of capabilities that are relevant in the context of IED security is necessary to develop MJIEDSPs and to guide future capability development efforts. To this end, the MJIEDSP process should explicitly identify target IED-specific capabilities and tasks for prioritized sites and the primary area of operations so that current preparedness levels can be compared with goals developed throughout this process.

Planning Actions:

5.1: Identify IED-related capabilities and tasks necessary to mitigate site-specific vulnerabilities.

Output: A consensus-based IED Security Task List for the overall planning area (NCAD leave behind)

Outcome: A common understanding of the tasks, which must be performed to achieve IED Security goals within the planning area

Metric: Increase in responders, leaders, and emergency managers who have identified, and reviewed the list of, key tasks which they or their organizations must perform

5.1: Identify IED-related capabilities and tasks necessary to mitigate site-specific vulnerabilities. A capability is a combination of elements (i.e. planning, personnel, organization and leadership, equipment and leadership, training, exercises and evaluations) needed to perform a set of identified critical tasks. The Target Capabilities List (TCL) (Figure 11), the Universal Task List (UTL), and NCAD provide a consolidated list of IED-specific capabilities and tasks to be reviewed for determining what actions to take to reduce vulnerabilities within your multi-jurisdiction area.

Figure 11: IED-security related TCL capabilities

TCL: IED-Security Related Capabilities
Information gathering and Recognition of Indicators and Warnings
Intelligence Analysis and Production
Intelligence/Information Sharing and Dissemination
Law Enforcement Investigation and Operations
CBRNE Detection
Critical Infrastructure Protection
On-Site Incident Management
Public Safety and Security Response
WMD/HAZMAT Response/Decontamination
Explosive Device Response Operations
Emergency Public Information and Warning

NCAD is a system which includes and on-site analysis tool based on the TCL and UTL used by OBP to assess the needs and current capabilities of jurisdictions throughout the Nation. Planners can use capability analysis reports from NCAD to review the tasks contained within each capability and identify the specific operational tasks and activities that need to be performed. The set of applicable tasks taken from NCAD may vary based upon the jurisdiction's threat and vulnerability profile. In addition, planners should review BZP plans, supplemental CIKR security plans, and scenario-specific response requirements for additional tasks and resources. Moreover, specific tasks should be considered as potential steady-state and threat-initiated actions identified in Steps 7 and 8.

Step 6: Assess Current Capabilities and Assets

After the specific IED-security tasks and capability requirements have been identified, planners should then work with DHS and the NCAD tool to assess their current levels of capability against the specific IED-security tasks and capability requirements identified in the previous step. When complete, this review will determine how well the jurisdictional area is currently able to perform the needed IED security tasks. The capabilities assessment will also identify gaps in capability and which capability elements may need to be improved or added to fill those gaps.

Planning Actions:

6.1: Assess current capabilities within primary area of operations

Output: Documentation of capability gaps within the planning area

Outcome: A common understanding of capability gaps in the planning area

Metric: Increase in jurisdictions' CIKR and soft targets for which gap analysis has been conducted; increase in grant submissions to improve IED Security capabilities

6.1: Assess capabilities within primary area of operations. Capabilities are delivered by appropriate combinations of properly planned, organized, equipped, trained personnel with a validated capability. The ability to deliver a given capability is measured by the performance of specific tasks.

A capabilities analysis will first identify the organizations within the planning area that are expected to perform specific critical tasks, including, but not limited to, public safety bomb squads, explosives detection canine teams, SWAT, and public safety dive teams. DHS will use the NCAD (Figure 12) to review these teams based upon the level of organization, training, equipment, and exercises, and compare them to the target levels of performance for each element identified in NCAD. The planner should revisit the Master Stakeholder List in the template and fill in each security partner's current capability levels as they move forward.

The capabilities analysis will reveal gaps in planning, organization, equipment, training, or exercising. Results are integrated into the comprehensive NCAD database for use in setting goals and measuring progress. The aggregated results in the NCAD database will inform national R&D, training and exercise priorities, while individual localities can use their localized results to inform their individual

Fiscal Year 2008 Homeland Security Grant Program (FY08 HSGP)

The development of a MJIEDSP also fulfills FY08 HSGP requirements by focusing State efforts on the IED threat.

FY08 HSGP states:
"Sates and Urban Areas should begin by implementing programs such as enhancing public and private sector IED awareness and reducing critical infrastructure/key resource (CIKR) and soft target explosive attack targets. Doing so will increase the likelihood that terrorist planning activities are recognized and reported, and deter attackes by reducing the attractiveness of potential targets. Additional programs such as implementing multi-jurisdictional explosive attack planning will ensure State and Urban Areas coordinate preventive and protective actions during steady-state and threat-initiated environments"

FY 2008 Homeland Security Grant Program: Program Guidance and Application Kit, U.S. Department of Homeland Security, January 2008, pg 5

and multi-jurisdiction investment priorities, and serve as investment justifications for grant programs.

Capabilities gaps may be first filled using Mutual Aid and Assistance Agreements (MAAs) between jurisdictions and then corrected through future investments linked directly to training, equipment, and exercises, necessary to maintain IED security. Because a capability can be delivered through multiple combinations of resources, jurisdictions seeking to correct shortfalls in capability can look to neighboring jurisdictions to provide some of the needed resources. MAAs between multiple jurisdictions enhance and complement the available resources of each partner jurisdiction. The process of searching out and creating MAAs, identified as a steady-state action in Step 7, also facilitates creative and flexible approaches to building capabilities, enabling jurisdictions to make better decisions about how they will develop and field capabilities moving forward. In the near-term, these agreements increase the level of capability that a given jurisdiction can deliver. In the longer-term, capability shortfalls identified in the capability analysis can be addressed using investments from available homeland security grant programs. In addition to equipment purchases, grant program funding can be used for training programs that increase the level of capability a given unit can provide, or to enhance exercise programs to demonstrate and improve planning, organization, and operations.

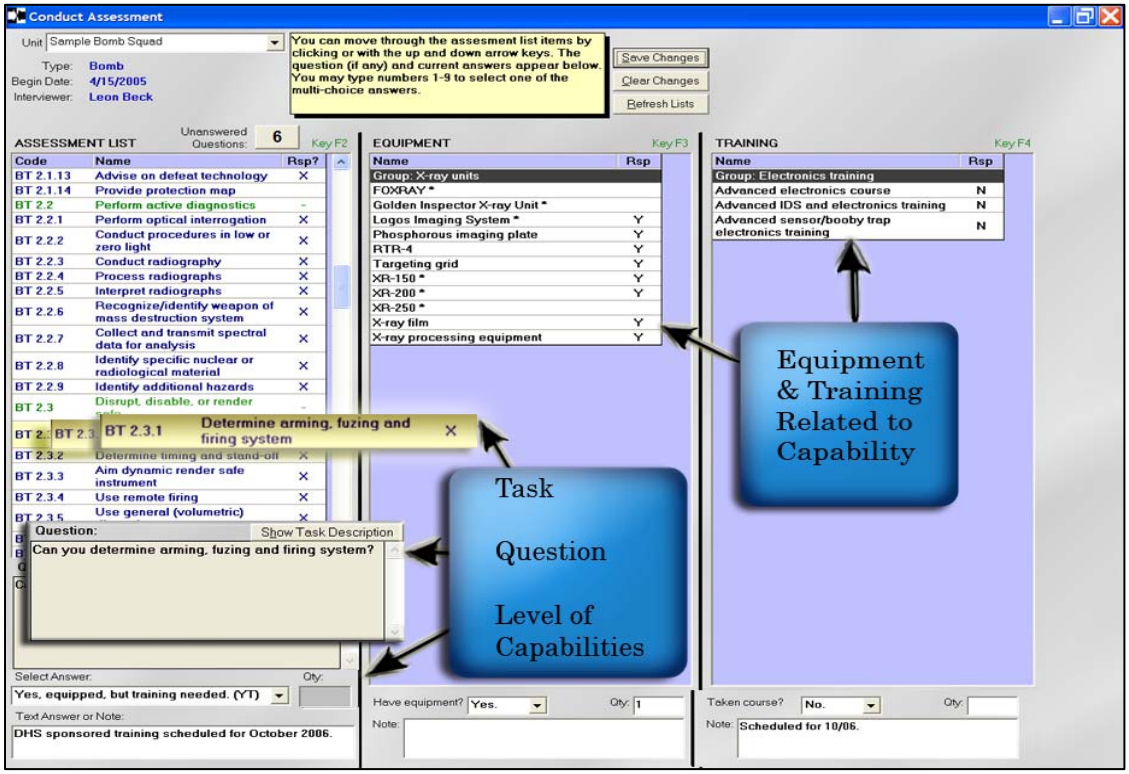

Figure 12: NCAD screenshot

Step 7: Identify Steady-State Actions

After each security partner's level of capability has been assessed, specific steady-state objectives and actions should be identified based on specific planning requirements identified in Step 5 to increase the planning area's overall level of IED security. Steady-state actions may include routine security procedures, or general preventive and protective measures to deter surveillance and attack planning or devalue a potential target. Implementing these tasks creates a random and unpredictable security presence across the multi-jurisdiction area to prevent IED attacks during their planning stages.

Planning Actions:

7.1: Define operational objectives for the primary area of operations

7.2: Identify steady-state security actions

7.3 Implement IED awareness campaigns

Output: An assigned list of steady-state security actions necessary to counter key threats and tactics

Outcome: Effective steady-state capabilities within the planning area

Metric: Increase in steady-state security presence across the multi-jurisdiction

7.1: Define operational objectives for the primary area of operations. Objectives describe what the multi-jurisdiction hopes to achieve to increase IED security. Having clearly stated objectives for steady-state environments allows emergency managers and responders to make intelligent decisions in the field in support of common goals for the multi-jurisdiction. Objectives for the multi-jurisdiction include:

- Devaluing potential targets (by creating contingency plans and system redundancies to reduce potential consequence of an attack),
- Detecting actions that may precede an attack (including the acquisition of bomb-making materials and surveillance of targets and potential terrorist hideouts;
- Deterring potential aggressors (by making the attack too difficult to execute by increasing the protective measures for a facility and within the planning area.

While these objectives are the same throughout the Nation, additional objectives may be identified based on the multi-jurisdiction's unique security needs.

7.2: Identify steady-state security actions. The vulnerabilities, required levels of capability, and current capability assessments inform the development of specific steady-state actions that increase the level of IED security within the multi-jurisdiction. Each action must relate to the three objectives mentioned above, and should be delineated between those that enhance the security posture of specific sites and those that can be applied to all sites within the primary area of operations. Most important, any actions developed must have clear definitions of activities, roles, and responsibilities to be performed to eliminate any confusion during operations. Figure 13 identifies specific steady-state action examples for both specific sites and the multi-jurisdiction. Appendix

A of the template provides an additional list of potential steady-state actions. The planner should record

Given limited resources, steady-state actions must take into account both the vulnerabilities of prioritized CIKR and soft targets and security partner's levels of capability. For example, while it would be ideal if police could be positioned within each subway station, limited law enforcement and the variances in threat levels for different targets require police to patrol those areas that have been prioritized.

Figure 13: Example steady-state actions

Site-specific steady-state actions examples for each objective	
Devalue	▪ Develop contingency and continuity of operation plans for the facility
Deter	▪ Conduct random, unpredictable security patrols at high-risk locations ▪ Conduct Buffer Zone Protection Planning ▪ Alternate access points ▪ Alternate access identification cards ▪ Deploy visible security cameras and motion censors
Detect	▪ Increase surveillance of specific facility or soft target to identify potential terrorists who may be conducting intelligence gathering
Multi-Jurisdiction steady-state action examples	
Devalue	▪ Develop mutual aid agreements and memoranda of understanding with surrounding jurisdiction so that the response to an incident is effective and timely ▪ Increase the training and exercising of security partners ▪ Effective positioning of assets to respond to threat initiated events
Deter	▪ Alternate canine and law enforcement patrol schedules
Detect	▪ Implement IED public awareness campaigns ▪ Provide Bombing Materials Awareness information for private sector through state and local law enforcement ▪ Develop relationships with local Joint Terrorism Task Forces (JTTFs) and Terrorism Early Warning Centers for increasing intelligence and information-sharing ▪ Work with the DHS National Infrastructure Coordination Center (NICC)5 to share CIKR related information and facilitate CIKR incident management throughout the multi-jurisdiction

7.3: Implement IED awareness campaigns. In a resource-constrained environment, it is not feasible to address every possible security concern. Understanding this challenge,

[5] The National Infrastructure Coordination Center NICC monitors the Nation's critical infrastructure and key resources (CIKR) on an ongoing basis. During an incident, the NOC-NICC provides a coordinating forum to share information across infrastructure and key resources sectors through appropriate information-sharing entities such as the Information Sharing & Analysis Centers and the Sector Coordinating Councils. To foster information sharing and coordination, private sector representatives from the CIKR may provide information to the NOC-NICC. U.S. Department of Homeland Security, (Washington, D.C. 2006), 7. For contact information, please contact your DHS Protective Security Advisor.

steady-state actions should include activities that focus on raising awareness and building communication and information-sharing relationships.

For example, law enforcement can inform private sector providers of chemicals or precursor materials used to manufacture homemade explosives (HME) or IED components of their potential use, and request them to notify authorities in the event of a suspicious purchase. DHS is currently developing a Bomb-Making Materials Awareness Program (BMAP) that State and local authorities should leverage when promoting IED awareness within their multi-jurisdiction.[6]

The Federal Transit Administration has developed the Transit Watch program that is also designed to encourage the active participation of transit passengers and employees in maintaining a safe transit environment.[7] Moreover, communities can develop their own public awareness campaigns that instruct the public to remain vigilant and notify local law enforcement in the even they see potential IEDs. These types of collaborative partnerships not only extend our reach into the community to identify threats at the earliest possible point, but also allow ample opportunities for relationship building and practicing coordination among entities for a coordinated IED response.

[6] For more information on BMAP, please contact the DHS Office for Bombing Prevention at OBP@dhs.gov.
[7] For more information on the Transit Watch program, please go to http://transit-safety.volpe.dot.gov/Security/TransitWatch/Default.asp.

Step 8: Identify Threat-Initiated Actions

IED threats present themselves on several levels of severity and specificity. This step includes developing a threat-rating system if such protocols are not already established, developing a concept of operations for a threat-initiated environment, and identifying specific sets of threat-initiated security actions for a facility or soft target and the primary area of operations.

Planning Actions:

8.1: Develop a standardized IED threat-rating system

8.2: Identify threat-initiated security actions

8.3: Define the concept of operations for managing an IED scenario

Outputs:	A standardized IED threat rating system; a consolidated list of threat-initiated security actions; and a concept of operations for a threat-initiated environment
Outcome:	An effective threat-initiated IED security capability within the planning area
Metric:	Increase in responders, leaders, and managers who understand and coordinate actions during threat-initiated environments

8.1: Develop a standardized IED threat rating system. Threat initiated security activities are a function of the severity and specificity of the threat. Therefore, plans for threat initiated security activities should include protocols for consistently categorizing potential threats. Planners can also estimate the scope and scale of the needed response based on the characteristics of each potential tactic and target, and the effects of each of the seven main types of IED attacks. This information can be used to quickly determine the resources needed to control the area, maintain public safety, and to manage the threat. Clear linkages should exist based on the specificity of the threat information and the resources needed to mobilize a reasonable response.

8.2: Identify threat-initiated security actions. Responding to a specific threat, whether the hazard has or has not been identified is critical to protecting lives and infrastructure. The actions that security partners take during this critical time often determine whether an attack achieves success or failure. Given limited resources, emergency managers should identify which threat-initiated actions to implement based on the type and specificity of the threat presented and available capabilities of security partners. In addition, threat-initiated actions should be determined on whether a threat has been made to a specific facility or set of facilities such as the financial sector, or if a less specific threat has been made to the multi-jurisdiction as a whole. Figure 14 provides examples of threat-initiated actions based for a specific facility or soft target. Moreover, security partners within the primary area of operations, if overwhelmed, should activate MAAs and MOUs, so that they may call upon surrounding jurisdictions to provide support. For example, if the jurisdictions within a primary area of operations do

not have enough trained canine detection teams or public safety bomb squads, they should be able to call upon the neighboring jurisdiction to provide teams if necessary.

Appendix B of the template provides additional threat initiated actions to choose from. Appendix C also provides a quick reference guide for identifying and assigning threat-initiated actions in response to an identified threat.

Figure 14: Example threat-Initiated Actions

Examples of threat-initiated actions for a specific facility or soft target:	
A threat has been made to a specific target or set of targets, or to the multi-jurisdiction as a whole	▪ Increase outside perimeter patrols ▪ Erect vehicle barriers ▪ Prohibit parking within or near site ▪ Close parking garages ▪ Conduct 24 hour perimeter security ▪ Increase number of law enforcement and explosive detection canine patrols throughout the entire multi-jurisdiction
Hazard has been identified (Appendix C of the Template)	▪ Assess the situation ▪ Identify the danger zone presented by the IED ▪ Establish control perimeter around device ▪ Evacuate surrounding area ▪ Establish Incident Command ▪ Activate MAAs and MOUs

8.3: Define the concept of operations for each IED scenario. The threat initiated portion of the MJIEDSP should define the basic concept of operations for a threat-initiated environment. First, roles and responsibilities of relevant response units should be predetermined based on the nature and specificity of the threat information that could potentially initiate a response. This portion of the plan should also describe general guidelines for standardized mobilization and deployment of response assets across response asset types and jurisdictional boundaries. In addition, guidelines should be determined for the sharing of information between security partners and the public. Finally, all security partners should update their specific operational procedures to comply with this concept of operations. The template provides the format for preparing the multi-jurisdiction's concept of operations. A general description of each section is described below.

A concept of operations should include the following:

I. **Threat-Rating System**
   This section should include your threat-rating system and should be used for initiating various threat-initiated actions based on the level of threat to your multi-jurisdiction area. For more information, see Planning Action 8.1.

II. **Basic Organization and Assignment of Responsibilities**
   This section should include the basic organizational elements required to manage an IED incident. All security partners should be listed with corresponding responsibilities and identified as the primary, coordinating, or supporting agency.

III. Incident Management

Incident management procedures should be consistent with both the basic principles of incident command outlined in the National Incident Management System and the processes for requesting additional support, including Federal aid as outlined in the National Response Framework. To this end, a clear process should be described that includes assessing the situation, locating the hazard (if possible), establishing a controlled area around the potential IED along the controlled zone, and creating of a unified command structure that integrates members of local law enforcement, public-safety bomb squads, emergency medical services, and State and Federal resources such as the FBI. In incidents involving multiple jurisdictions, a single jurisdiction with multi-agency involvement or multiple jurisdictions with multi-agency involvement, unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

IV. Information Management

Since each jurisdiction within a planning area may have different intelligence resources at its disposal, security partners may not have equal access to threat information. For example, some jurisdictions may be able to obtain intelligence on IED threats through an area Joint Terrorism Task Force (JTTF) or Fusion Center, while others may rely on local law enforcement for threat information. The MJIEDSP must therefore provide guidelines and procedures for sharing intelligence and threat information among the jurisdictions in a given planning area.

When a specific threat emerges, it will be critical for law enforcement and other responders to have access to intelligence and information on potential perpetrators, threats, and terrorist TTPs. To ensure that this information is available, the MJIEDSP should include general guidelines for retrieving relevant information on both threats and facilities.

In addition to intelligence about perpetrators, threats, and terrorist TTPs, security partners must also have access to information about the facilities and locations of concern within their planning area. Law enforcement and other responders should be able to access the assessments developed and compiled during the MJIEDSP process. For example, if a specific threat presents itself against a facility for which a vulnerability assessment or BZP has been developed, procedures should exist that ensure the assessment information is available to incident commanders. The threat-initiated portion of the MJIEDSP should describe the process for identifying available response assets and positions via NCAD or some other support tool.

V. Emergency Public Information

General procedures should be outlined for notifying the public of potential threats, directing their actions, and keeping them informed as the situation progresses. Most important, any information should discuss evacuation procedures and/or shelter-in place policies.

VI. Mutual Aid and Assistance Agreements (MAAs), Memoranda of Understanding (MOUs)

Finally, the threat-initiated portion of the MJIEDSP should also define guidelines for triggering MAAs and MOUs in a timely and appropriate manner. Ideally, the

plan will include an index of existing agreements and conditions under which each can be triggered, and will define how the additional resources made available by the MAA will be integrated into ongoing response operations for each type of incident.

Step 9: Validate Plan

The next step in the Multi-Jurisdiction IED Security development process is the review and validation of the plan through a multi-jurisdiction IED scenario exercise. This exercise will provide an opportunity for the jurisdictions' emergency responders and homeland security officials to practice and assess their collective IED security capabilities. Once the initial exercise is complete, routine exercises should be incorporated into the plan maintenance process to ensure that the MJIEDSP accurately reflects the needs of the IED security environment for the planning area.

Planning Actions:

9.1: Conduct multi-jurisdiction IED exercise to practice and assess the MJIEDSP

9.2: Implement post-exercise corrective actions to improve and finalize the MJIEDSP

Output: An initial MJIED table top planning exercise

Outcome: An initial validated MJIEDSP via a multi-jurisdiction IED security exercise

Metric: Increase in responders, leaders, and emergency managers who have reviewed and practiced their roles in the MJIEDSP

9.1: Conduct multi-jurisdiction IED exercise to practice and assess the MJIEDSP. Each planning area should validate its MJIEDSP through an exercise that engages security partners in all participating jurisdictions. The exercise should conform to Homeland Security Exercise and Evaluation Program (HSEEP) standards and be evaluated on the relevant aspects of the Target Capabilities List (TCL). The goals of the exercise and the subsequent evaluation are to validate areas of strength, identify opportunities for improvement, and establish how prepared the region is in order to prevent, protect against, respond to, and/or recover from a terrorist IED attack.

The validation exercise can be modified to meet the varying needs and capabilities of the participating jurisdictions, employing many scenarios and exercise types. Planners should refer to the HSEEP reference volumes for guidance on the design, development, and management of exercises.[8] The content of the multi jurisdiction IED exercise should incorporate the specific needs of the issues of the jurisdiction, providing a realistic scenario that exercises as many security partners as possible.

9.2: Implement post-exercise corrective actions to improve and finalize the MJIEDSP. The results and lessons learned from the exercise will provide valuable insight into the strengths and weaknesses of the plan and allow planners to take corrective actions to improve the MJIEDSP. The post-exercise evaluation process includes a formal exercise evaluation, analysis of lessons learned, and drafting of an After-Action Report/Improvement Plan (AAR/IP). Planners and exercise evaluators

[8] Homeland Security Exercise Evaluation Program Reference Volumes I-IV can be found at the HSEEP website [www.hseep.dhs.gov]

should refer to the HSEEP reference volumes for more information about the formal exercise evaluation process. The AARs and other analyses will allow planners to identify areas requiring improvement and adjust the plan accordingly.

Step 10: Establish Plan Maintenance Process

Multi-Jurisdiction IED Security Plans must be evaluated and revised on an ongoing basis to reflect changing threat environments, new policies and guidance, legislative changes, fluctuations in planning area resources and capabilities, and procedural changes based on lessons learned from exercises and actual events. This step establishes procedures for changing the content of a given MJIEDSP.

Planning Actions:

10.1 Establish procedures for conducting regular plan reviews of MJIEDSP

10.2 Establish procedures for proposing and coordinating plan changes

Output: Processes for reviewing, updating, and changing the MJIEDSP

Outcome: A MJIEDSP that accurately reflects changing threat environments and planning area capabilities

Metric: Increase in frequency of plan updates

10.1 Establish procedures for conducting regular plan reviews of MJIEDSP. Once a MJIEDSP is finalized, planners should update the document on at least an annual basis. Collaborative and regular review will keep the plan current and relevant, incorporate new partners or processes, and retires obsolete content. Given the dynamic and adaptable nature of the IED threat, it is critical that this plan remains as useful and up-to-date as possible.

Plan reviews should be based on lessons learned gathered from drills, training, and exercises held on a regular basis or responses to actual IED incidents in the planning area. The lessons learned and best practices gathered from these exercises and incidents should lead to corrective actions and updates to the plan. These updates may include changes to the plan's steady-state and threat-initiated actions. In addition, any changes made to the TCL's performance metrics would also be taken into consideration for changing steady-state and threat-initiated actions. After corrective actions have been implemented, a tabletop exercise should be scheduled as a follow-up activity to ensure that the corrective actions do in fact address the issues identified during the exercise or incident.

Where applicable, it may be beneficial to observe or learn about the findings of other multi-jurisdiction areas' review processes. Sharing lessons learned reduces the burden on individual planning areas and speeds the process of implementing newly identified requirements throughout the nation.

10.2 Establish procedures for proposing and coordinating plan changes. In order to keep the plan as up-to-date as possible, planners must establish set procedures for proposing and implementing changes. These procedures should include when, how, and with what frequency changes can be made and who presides over the process.

Any security partner participating in the planning process may propose a change to the plan. Changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, state or local homeland security plans, or regulation. The planning group, whether it be the jurisdiction's office of emergency management or law enforcement, is responsible for coordinating all proposed modifications to the plan with primary and support partners from throughout the planning area, as required. The planning group will coordinate review and approval for proposed modifications through locally-determined processes as required.

Appendix A –Multi-Jurisdiction IED Security Plan Checklist

Step 1: Identify the Planning Area		
	1.1 Identify the primary area of operations	☐
	1.2 Identify neighboring jurisdictions that may provide assistance	☐
Step 2: Identify Facilities or Locations of Concern		
	2.1 Identify Critical Infrastructure and Key Resources (CIKR) assets, systems, and networks within the primary area of operations	☐
	2.2 Identify other facilities or locations of concern, such as “soft targets” and other vulnerable sites within the primary area of operations	☐
	2.3 Prioritize identified facilities and soft targets according to their criticality	☐
Step 3: Identify Security Partners		
	3.1 Identify potential security partners for both your primary area of operations and neighboring jurisdictions determined during Step 1	☐
	3.2 Determine the individuals from each agency or discipline that should participate in the planning process	☐
Step 4: Identify Site-Specific Concerns		
	4.1 Identify viable and likely IED tactics, techniques, and procedures that could be used to threaten the facility or soft target	☐
	4.2 Conduct a vulnerability analysis of each prioritized C/KR and soft target	☐
Step 5: Identify IED Security Needs		
	5.1 Identify capabilities and tasks necessary to mitigate site-specific vulnerabilities	☐
Step 6: Assess Capabilities and Assets		
	6.1 Assess current capabilities within MJIEDSP primary area of operations	☐
Step 7: Identify Steady-State Actions		
	7.1 Define operational objectives for your primary area of operations	☐
	7.2 Identify steady-state security actions	☐
	7.3 Implement IED awareness campaigns	☐
Step 8: Identify Threat-Initiated Actions		
	8.1 Develop a standardized IED threat-rating system	☐
	8.2 Identify threat-initiated actions	☐
	9.3 Define concept of operations for managing an IED scenario	☐
Step 9: Validate Plan		
	9.1 Conduct multi-jurisdiction IED exercise to practice and assess the MJIEDSP	☐
	9.2 Implement post-exercise corrective actions to improve and finalize the MJIEDSP	☐
Step 10: Establish Plan Maintenance Processes		
	10.1 Establish procedures for conducting regular plan reviews of MJIEDSP	☐
	10.2 Establish procedures for proposing and coordinating plan changes	☐

THIS PAGE IS INTENTIONALLY BLANK

DRAFT