

**MULTISERVICE
TACTICS,
TECHNIQUES, AND
PROCEDURES FOR
INSTALLATION
CBRN DEFENSE**

**FM 3-11.34
MCWP 3-37.5
NTTP 3-11.23
AFTTP(I) 3-2.33**

NOVEMBER 2007

DISTRIBUTION RESTRICTION:
Approved for public release;
distribution is unlimited.



FOREWORD

This publication has been prepared under our direction for use by our respective commands and other commands as appropriate.



THOMAS W. SPOEHR
Brigadier General, USA
Commandant
U.S. Army Chemical School



JAMES F. AMOS
Lieutenant General, USMC
Deputy Commandant
Combat Development and
Integration



T.L. DAVISON
Captain, USN
Acting Commander
Navy Warfare Development Command



ALLEN G. PECK
Major General, USAF
Commander
Headquarters Air Force Doctrine
Center

This publication is available at Army Knowledge Online <www.us.army.mil>, the General Dennis J. Reimer Training and Doctrine Digital Library <<http://www.train.army.mil>>, and the e-Publishing web site <www.e-publishing.af.mil>.

PREFACE

1. Scope

This multiservice publication represents a significant revision to the August 2000 publication by expanding the scope from theater-based tactical sites to installations found in both foreign and domestic locations. It is designed for military commanders and personnel responsible for chemical, biological, radiological and nuclear (CBRN) defense planning at installations in the continental United States (CONUS) and outside the continental United States (OCONUS). The term “installation” will be used henceforth when referring to fixed sites, ports, and airfields in this manual. These personnel may be responsible for deliberate or crisis planning and may be required to execute plans across the conflict spectrum. This publication provides doctrine and tactics, techniques, and procedures (TTP) for planning, resourcing, and executing CBRN defense for various military installations as part of an overarching installation protection program. The chapters present a doctrinal foundation, and specific TTP are included in the appendixes. This manual incorporates the joint doctrine elements for combating weapons of mass destruction (WMD), to include counterproliferation passive defense functions of CBRN sense, shape, shield, and sustain. It also ties installation CBRN defense to consequence management doctrine. During military operations, this publication is subordinate to current joint publications (JPs) addressing this topic. This document incorporates the following key guidance:

- National Response Plan (NRP).
- National Incident Management System (NIMS).
- Department of Defense Instruction (DODI) 6055.1.
- DODI 2000.16.
- DODI 2000.18.
- DODI 6055.06.
- Department of Defense (DOD) 6055.06-M.
- Department of Defense Directive (DODD) 2000.12.
- Service-specific policies addressing emergency response to CBRN incidents at CONUS installations, such as—
 - AF 10-25-series manuals.
 - Chief of Naval Operations Instruction (OPNAVINST) 3440.17.
 - OPNAVINST 5100.23G.

2. Purpose

The purpose of this publication is to provide commanders, staffs, key agencies, and service members with a key reference for planning and conducting CBRN defense of installations. It provides the tools for CBRN defense personnel to implement active and passive CBRN sense, shape, shield, and sustain measures. It also serves as a key source

document for refining existing service publications, training support packages, training center exercises, and service school curricula.

3. Application

This publication is designed for use at the operational and tactical levels but has implications at the strategic level in the implementation of CBRN defense on installations supporting strategic objectives. The document will support command staff planning in preparing for and conducting CBRN defense operations on installations as a part of an overarching installation protection program. The manual also provides guidance to installation leaders and personnel for implementing CBRN defense.

4. Implementation Plan

Participating service command offices of primary responsibility (OPRs) will review this publication, validate the information, and reference and incorporate it into service and command manuals, regulations, and curricula as follows:

Army. The United States Army (USA) will incorporate the procedures in this publication in USA training and doctrinal publications as directed by the Commander, United States Army Training and Doctrine Command (TRADOC). Distribution is according to Department of the Army (DA) Form 12-99-R, *Initial Distribution (ID) Requirements for Publications*.

Marine Corps. The United States Marine Corps (USMC) will incorporate the procedures in this publication in training and doctrinal publications as directed by the Commanding General (CG), Marine Corps Combat Development Command (MCCDC). Distribution is according to the USMC publications distribution system.

Navy. The United States Navy (USN) will incorporate the procedures in this publication in training and doctrinal publications as directed by the Commander, Navy Warfare Development Command (NWDC). Distribution is according to DOD 4000.25-1-M.

Air Force. The United States Air Force (USAF) will validate and incorporate appropriate procedures according to the applicable governing directives. It will develop and implement this and other CBRN multiservice tactics, techniques, and procedures (MTTP) publications through a series of USAF manuals providing service-specific TTP. Distribution is according to the USAF publication distribution system.

5. User Information

a. The United States Army Chemical School (USACMLS) developed this publication with the joint participation of the approving service commands.

b. We encourage recommended changes for improving this publication. Please reference changes by specific page and paragraph, and provide a rationale for each recommendation. Send comments and recommendations directly to—

Army

**Commandant
U.S. Army Chemical School
ATTN: ATSN-TD
464 MANSCEN Loop, Suite 2661
Fort Leonard Wood, MO 65473-8926
DSN 676-7364; COMM (573) 563-7364
Web site: <<https://www.us.army.mil/>>**

Marine Corps

**Deputy Commandant for
Combat Development and Integration
ATTN: MCCDC CDD MID DCB C116
3300 Russell Road Suite 204
Quantico, VA 22134-5021
DSN 278-6233; COMM (703) 784-6233
Web site: <<https://www.doctrine.usmc.mil/>>**

Navy

**Commander
Navy Warfare Development Command
ATTN: N5
686 Cushing Road
Newport, RI 02841-1207
DSN 948-4201; COMM (401) 841-4201
Web site: <<https://www.nko.navy.mil/>>**

Air Force

**Headquarters Air Force Doctrine Center
ATTN: DJ
155 North Twining Street
Maxwell AFB, AL 36112-6112
DSN 493-7442; COMM (334) 953-7442
Web site: <<https://www.doctrine.af.mil/>>**

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

***FM 3-11.34
MCWP 3-37.5
NTTP 3-11.23
AFTTP(I) 3-2.33**

FM 3-11.34 U.S. Army Training and Doctrine Command
Fort Monroe, Virginia
MCWP 3-37.5 Marine Corps Combat Development Command
Quantico, Virginia
NTTP 3-11.23 Navy Warfare Development Command
Newport, Rhode Island
AFTTP(I) 3-2.33 Headquarters Air Force Doctrine Center
Maxwell Air Force Base, Alabama

6 November 2007

**Multiservice Tactics, Techniques, and Procedures
for
Installation CBRN Defense
TABLE OF CONTENTS**

	Page
EXECUTIVE SUMMARY	viii
CHAPTER I INTRODUCTION	I-1
Fundamentals of Installation CBRN Defense	I-1
Operational Environment.....	I-2
Installation CBRN Defense Framework	I-3
CHAPTER II INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENSE PLANNING	II-1
Overview	II-1
Installation Command and Staff Responsibilities.....	II-1
Operational Environment Assessment	II-3
Vulnerability Assessment.....	II-9
Commander's Guidance	II-11
Plan Development	II-11

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This manual supersedes FM 3-11.34/MCWP 3.37.5/NTTP 3-11.23/AFTTP(I) 3-2.33,
29 September 2000.

	Page
CHAPTER III	INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENSE PREPARATION III-1
	Overview III-1
	Acquisition of Necessary CBRN Defense Equipment III-2
	Preparation of Facilities III-3
	Education and Training III-4
	Coordination, Monitoring, and Reporting Requirements III-8
	Conducting Response Exercises III-10
	Reassess Capabilities and Identify Remaining Vulnerabilities III-11
	Threat Advisory Systems III-12
CHAPTER IV	INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR RESPONSE IV-1
	Fundamentals of Installation Response IV-1
	Tiered Response IV-4
	Emergency Support Functions and Roles IV-9
	Emergency Communications (Warning and Reporting) IV-9
	Common Operational Picture (COP) IV-11
	Transition to Recovery and Immediate Mitigation IV-12
CHAPTER V	INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR RECOVERY V-1
	Fundamentals of Recovery V-1
	Unique Operational Environment Considerations V-3
	Recovery Phase Command and Control V-4
	Mitigating CBRN Hazard Effects V-6
APPENDICES	
	A. Installation Chemical, Biological, Radiological, and Nuclear Plan Development A-1
	B. Emergency Support Function (ESF) Manager Roles B-1
	C. Installation Chemical, Biological, Radiological, and Nuclear Checklists C-1
	D. Force Health Protection Capabilities, Restrictions, and Considerations D-1
	E. Collective Protection and In-Place Protection E-1
	F. Split Mission-Oriented Protective Posture Operations F-1
	G. Civilian and Contractor Chemical, Biological, Radiological, and Nuclear Defense Considerations G-1

H. Responsibilities for Installation Chemical, Biological,
Radiological, and Nuclear Defense H-1

I. Chemical Contamination Control for Airlift Operations I-1

J. Installation Chemical, Biological, Radiological, and
Nuclear Defense Capability Packages J-1

REFERENCESReferences-1

GLOSSARYGlossary-1

INDEX.....Index-1

FIGURES

Figure I-1. Installation CBRN Defense Framework I-4

Figure II-1. Planning Phase for Installation CBRN Defense II-1

Figure II-2. Vulnerability Assessment During the
Planning Phase II-10

Figure II-3. Military Decision-Making Process II-12

Figure III-1. Preparation Phase for Installation
CBRN Defense.....III-1

Figure III-2. Vulnerability Assessment During the
Preparation Phase.....III-12

Figure IV-1. Response Phase for Installation CBRN
Defense IV-1

Figure IV-2. Installation Response Example..... IV-3

Figure IV-3. ICS Major Management Functions..... IV-5

Figure IV-4. Installation Incident Command System..... IV-7

Figure V-1. Recovery Phase for Installation CBRN Defense..... V-1

Figure V-2. Contamination Marking Signs V-10

Figure A-1. Installation CBRN Defense Plan Format A-1

Figure A-2. Sample Installation CBRN Defense Plan A-6

Figure C-1. Sample Installation-Level CBRN Coordination
With a Tenant or Transient Unit..... C-9

Figure C-2. Tenant or Transient Unit Level CBRN
Coordination With an Installation C-13

Figure E-1. SIP Sign for Posting Outside Rooms
or Buildings E-10

Figure F-1. Sector or Zone Identification (Notional Example) F-1

Figure F-2. Sample Base Sectoring with Split MOPP Levels.....F-2

Figure F-3. Transition Point DiagramF-6

Figure G-1. Evacuation Processing Flow of Personnel G-6

Figure I-1. Basic Flowchart for In-Flight Decontamination..... I-10

Figure I-2. Sample Supervisor Checklist..... I-17

Figure I-3. Sample Assistant Checklist I-18

	Page
Figure I-4. Sample Aircrew Decontamination Checklist	I-19
Figure I-5. Sample Mission-Essential Loading Checklist.....	I-20
Figure I-6. Sample Mission Support Loading Checklist	I-21
Figure I-7. Sample Retrograde Loading Checklist.....	I-22
Figure I-8. Sample In-Flight Decontamination Checklist for Maximum Decontamination of Payload	I-22
Figure I-9. Sample In-Flight Decontamination Checklist	I-23
for Minimum Contamination of Aircraft	

TABLES

Table II-1. Potential TIM Hazard Sources	II-4
Table II-2. CBRN Threat Levels	II-5
Table II-3. Installation Zoning Principles.....	II-5
Table III-1. FPCONs	III-13
Table III-2. CBRN Threat Levels	III-14
Table IV-1. Flow of Events for Installation CBRN Response	IV-2
Table IV-2. Standardized Alarm Signals for the US and its Territories and Possessions	IV-10
Table IV-3. Standardized Alarm Signals for OCONUS Bases and Stations Subject to CBRN Attacks.....	IV-11
Table A-1. Technical Reach-Back Contact Information	A-13
Table B-1. Sample ESF Manager Roles	B-1
Table C-1. Planning and Preparatory Actions.....	C-1
Table C-2. Response Actions.....	C-4
Table C-3. Recovery Actions	C-6
Table E-1. General Protection-In-Place Options	E-3
Table E-2. Establishing an SIP Program.....	E-7
Table E-3. SIP Notification and Response Procedures	E-8
Table F-1. Processing Through a CCA.....	F-5
Table G-1. Sample CBRN Tasks	G-4
Table G-2. Sample First Aid Tasks	G-4
Table I-1. Generic Matrix for Aircraft/Payload Handling.....	I-16

EXECUTIVE SUMMARY

Multiservice Tactics, Techniques, and Procedures for Installation CBRN Defense

Chapter I Introduction

Chapter I describes the various types of installations and introduces the implication of their location with respect to the limits and extents of the installation commander's authority. It presents complementary tactical CBRN doctrine as it relates to installation CBRN defense. It also introduces the factors of the operational environment that impact installation CBRN defense operations. The four major phases representing the installation CBRN defense framework are presented—planning, preparation, response, and recovery. Finally, it describes the relationship of installation CBRN defense procedures to those involving CBRN consequence management, for which doctrine and TTP are found in the complementary tactical CBRN doctrine.

Chapter II Installation CBRN Defense Planning

Chapter II presents installation command and staff responsibilities in planning for CBRN defense. It focuses on critical operational environment assessments—threat, physical, information, and political. Vulnerability assessment is related to the planning phase, as well as the importance of implementing commander's guidance—specifically with regard to risk management. Finally, it promotes the implementation of the military decision-making process as a method by which to integrate CBRN defense planning into the overall installation protection plan.

Chapter III Installation CBRN Defense Preparation

Chapter III extends the planning phase by describing the implementation of vulnerability reduction measures consistent with command guidance through the vulnerability assessment process. It describes coordination measures, task organization, equipping, training and certification, exercises, readiness evaluations, and the use of threat advisory systems.

Chapter IV

Installation CBRN Response

Chapter IV discusses immediate response measures following a CBRN incident. It describes various responder classifications and how they are employed in a tiered response fashion. Organization and implementation of various responder operations centers are presented, as well as forms of emergency communications—warning and reporting to notify.

Chapter V

Installation CBRN Recovery

Chapter V presents installation commander recovery operations within the extent of his own available organic and precoordinated resources. It emphasizes immediate response and mitigation measures to restore critical functions to their preincident capability. It presents methods to mitigate the effects of a CBRN incident and describes the transition to plan revision upon reassessment and lessons learned. Finally, it describes the relationship between installation CBRN defense recovery and CBRN consequence management operations as differentiated by the capabilities immediately at the installation commander's disposal without external coordination.

Appendices

Appendix A provides TTP for installation CBRN defense planning, to include a plan format, a sample plan, and technical reach-back assets.

Appendix B describes the emergency support functions from the National Response Plan in greater detail.

Appendix C provides detailed checklists for all phases of installation CBRN defense operations.

Appendix D discusses force health protection measures in greater detail than presented in the chapter material.

Appendix E addresses collective protection and in-place protection TTPs and their integration into the installation CBRN defense plan.

Appendix F introduces the installation commander's option to exercise split MOPP and installation zoning as TTP to maintain critical installation functions after a CBRN incident.

Appendix G describes the unique relationships, requirements, and responsibilities inherent when integrating civilians and contract personnel into the CBRN defense plan.

Appendix H provides detailed responsibilities for installation commanders, staffs, responders, tenant units, and transient units.

Appendix I addresses contamination control for airlift operations.

Appendix J describes installation capability packages as a method to prioritize the installation CBRN defense capabilities in a tiered approach based on mission.

PROGRAM PARTICIPANTS

The following commands and agencies participated in the development of this publication:

Joint

Joint Requirements Office, 401 MANSCEN Loop, Suite 1309, Fort Leonard Wood, MO 65473

Army

United States Army Chemical School, 464 MANSCEN Loop, Suite 2617, Fort Leonard Wood, MO 65473

United States Army Medical Department Center and School, 1400 E. Grayson Street, Fort Sam Houston, TX 78234

Marine Corps

United States Marine Corps Combat Development Command, 3300 Russell Road, Suite 204, Quantico, VA 22134-5021

Navy

United States Navy Warfare Development Command, 686 Cushing Road, Sims Hall, Newport, RI 02841

Air Force

HQ Air Force Doctrine Center, ATTN: DJ, 155 North Twining Street, Maxwell AFB, AL 36112-6112

United States Air Force Civil Engineer Support Agency, 139 Barnes Drive, Suite 1, Tyndall AFB, FL 32403

Chapter I

INTRODUCTION

1. Fundamentals of Installation CBRN Defense

This chapter establishes the environment for CBRN defense of installations. It provides the terms of reference for CBRN defense of installations and illustrates the integration of complementary tactical CBRN passive defense MTTP relate to this manual. The chapter also addresses the operational environment for installations and the installation CBRN defense framework – plan, prepare, respond, and recover. Finally, it describes the transition potential from installation CBRN defense operations to CBRN consequence management operations.

a. Terms of Reference.

(1) Installation. JP 1-02 defines an installation as a grouping of facilities, located in the same vicinity, which supports particular functions. Examples of installations include, but are not limited to the following:

- Posts or bases.
- Ports (sea or air).
- Airfields.
- Base clusters.
- Staging areas.
- Command and control nodes.
- Logistics nodes.
- Other facilities or fixed sites to include expeditionary bases and camps.

(2) Geographic Locations. US military installations support operational forces in domestic and foreign environments. The particular location of the installation is critical in determining the laws or regulations that must be applied, as well as the level of military authority the installation commander may have in determining response actions – to include the level of personal protection for the response force.

(a) Domestic Locations. DODI 2000.21 lists the following as domestic locations: the continental United States (CONUS), Alaska, Hawaii, the Commonwealth of Puerto Rico, the US Virgin Islands, US territories of Guam, American Samoa, Jarvis Island, the Commonwealth of the Northern Marianas Islands, the Freely Associated States of Micronesia, the Republic of Palau, the Republic of the Marshall Islands, and the US possessions of Wake Island, Midway Island, Johnson Island, Baker Island, Howland Island, Palmyra Atoll, and Kingman Reef.

(b) Foreign Locations. DODI 2000.21 defines foreign locations as any geographic area not reflected in the definition of domestic.

b. Complementary Tactical CBRN Doctrine.

(1) *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Defense Operations* provides principles for the

installation CBRN staff on their roles and responsibilities in executing installation CBRN defense.

(2) *Multiservice Tactics, Techniques, and Procedures for CBRN Contamination Avoidance* addresses the principle of contamination avoidance and describes the CBRN Warning and Reporting System (CBRNWRS) which may be integrated into installation CBRN defense actions.

(3) *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Protection* describes methods for protecting personnel and equipment from CBRN hazards in a tactical environment, and levels of personal protection.

(4) *Multiservice Tactics, Techniques, and Procedures for CBRN Decontamination* provides decontamination guidance for personnel, equipment, facilities, and terrain.

(5) *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Vulnerability Assessment* provides planning guidance for conducting vulnerability assessments that may be applicable to installation CBRN defense planning and preparation phases.

(6) *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Reconnaissance* provides principles and tactics, techniques, and procedures (TTP) for detection and identification that may be applied to the installation CBRN protection plan.

(7) *Multiservice Tactics, Techniques, and Procedures for Biological Surveillance* provides principles and TTP for biological surveillance operations that may be applied to the installation CBRN defense plan.

(8) *Health Service Support in a Chemical, biological, radiological, and nuclear Environment* provides supporting medical doctrine, to include patient decontamination procedures.

2. Operational Environment

a. **Threat.** There are common threat considerations that apply to military installations during military operations ranging from stable peace to full scale war. Installations will likely receive intelligence summaries that provide information on the local or regional threat. CBRN threats and hazards can range from adversarial actions to man-made incidents/accidents to natural disasters. A key component of the threat assessment is to determine whether a deliberate capability exists with a corresponding intent.

b. **Physical Environment.** Key components of the physical environment include terrain and weather and their effects as well as the geographic framework that influences the installation commander's plan and ability to exercise his authority.

(1) **Terrain.** Topography, soil and surface type, and vegetation directly impact CBRN operations on installations.

(2) **Weather.** Precipitation, winds, air stability, humidity, and temperature are among those factors that also impact CBRN operations on installations.

(3) **Geographic Framework.** The commander's plan for installation CBRN defense must encompass the assigned area of operations (AO) and the associated areas of interest. The area of operations establishes the boundaries within which the installation commander operates, and controls response actions. The area of interest represents the environment external to the AO for which the installation commander must maintain situational awareness, and may include surrounding communities and civil authorities with whom the installation commander establishes agreements for coordinated notification, response, and recovery operations.

c. **Information Environment.** The installation commander strives to achieve situational awareness and understanding by integrating technology with capabilities of military and civil authorities. The installation commander determines sources of information – to include intelligence – and appropriate stakeholders for information sharing. Further, a CBRN incident may require notification procedures among military commanders and civil authorities that must be based on common agreements and pre-established methods.

d. **Political Environment.** Military authority, jurisdictional authority, established agreements, and local customs are among the important political, legal, and cultural issues for the installation commander. Installation commanders must consider cultural, ethnic, and religious attitudes and behaviors that may impact operations.

3. Installation CBRN Defense Framework

a. **Installation Defense.** Installation defense consists of four phases that can occur sequentially or simultaneously as shown in Figure I-1 and described in Chapters II through V. The four phases are:

- Planning.
- Preparation.
- Response.
- Recovery.

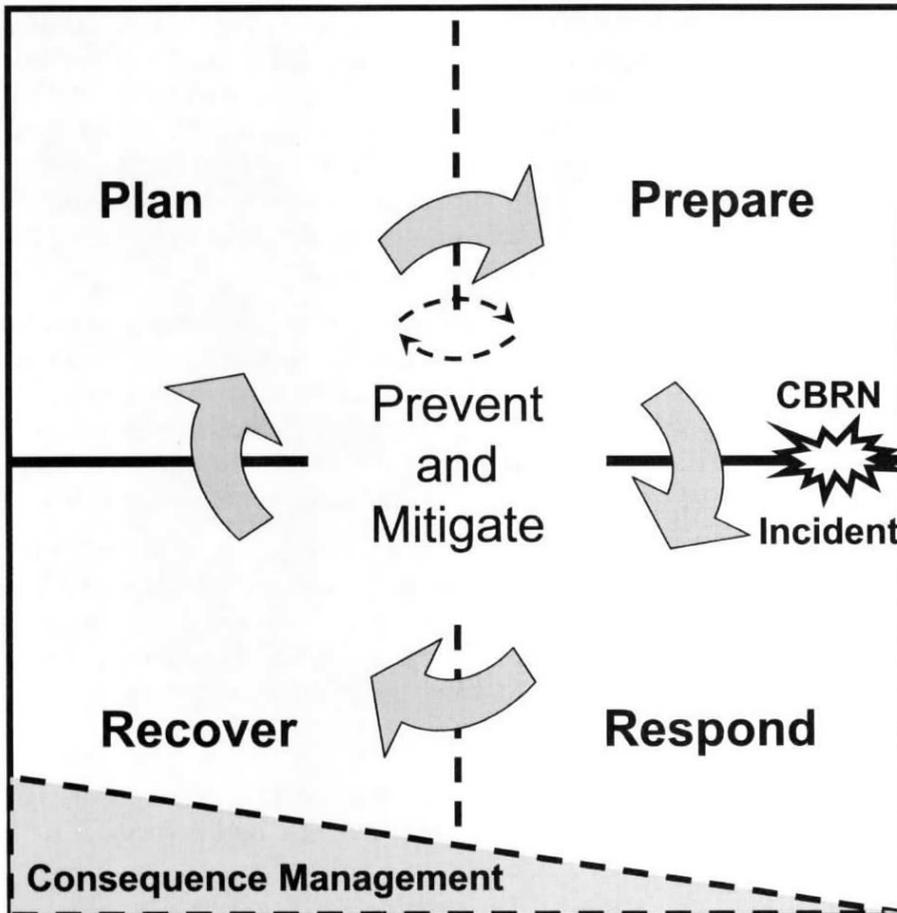


Figure I-1. Installation CBRN Defense Framework

(1) **Planning Phase.** Planning is based upon assessment of the operational environment and enables commanders to identify minimum standards for training, organizing, equipping, and protecting resources. The plan drives preparation and facilitates response and recovery operations. Chapter II discusses the planning phase in more detail.

(2) **Preparation Phase.** Preparation implements the approved plan and relevant agreements to increase readiness through training, exercises, and certification. Vulnerability reduction measures are also initiated to support prevention and mitigation functions. Chapter III discusses the preparation phase in more detail.

(3) **Response Phase.** The response phase addresses the short-term, direct effects of an incident. Response measures include those actions taken to save lives, protect property, and establish control. Chapter IV discusses the response phase in more detail.

(4) **Recovery Phase.** The focus of recovery is on restoring mission capability and essential public and government services interrupted by the CBRN incident. The recovery phase also includes completing the mitigation of the immediate hazard. Chapter V discusses the recovery phase in more detail.

b. **Consequence Management.** The CBRN aspects of consequence management include those actions taken to manage and mitigate the effects of a CBRN attack or incident and restore essential operations and services by employing capabilities beyond those immediately available to the installation. The *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Aspects of Consequence Management* provides more information for CBRN incidents in which the installation commander's immediate and coordinated response resources are insufficient to complete response and recovery operations.

This page intentionally left blank.

Chapter II

INSTALLATION CBRN DEFENSE PLANNING

1. Overview

Planning for installation CBRN defense and the development of the installation CBRN defense plan begins with the assessment of the operational environment and installation command and staff assessments (see Figure II-1). Application of the military decision making process (MDMP) matures these assessments and estimates into a published installation CBRN defense plan. The installation CBRN defense plan requires continuous assessment over time to integrate changes in threat, vulnerability assessments, capabilities, and command relationships with civil authorities. The installation CBRN defense plan may be a stand-alone document or an addendum to an existing installation protection plan (IPP). The installation commander and his staff have the primary responsibility for developing the installation CBRN defense plan.

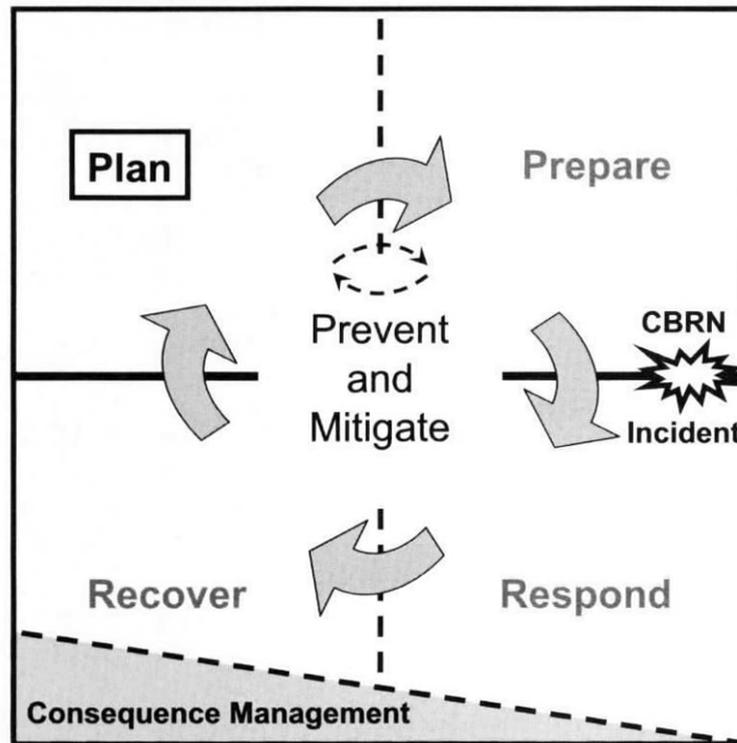


Figure II-1. Planning Phase for Installation CBRN Defense

2. Installation Command and Staff Responsibilities

The commander and his staff are responsible for establishing the installation's CBRN defense plan, to include threat assessment, vulnerability analysis and reduction, emergency response, and immediate recovery operations across the range of possible CBRN hazards. A summary of tasks for installation commanders and staffs is provided below. A comprehensive listing of responsibilities, to include CBRN responders and tenant/transient units is provided in Appendix H.

- a. The responsibilities of all installation commanders include:
- Develop a comprehensive installation CBRN defense plan.
 - Train, rehearse, and exercise the CBRN defense plan.
 - Allocate installation activities and resources to support the installation CBRN defense plan.
 - Continuously assess and improve the installation CBRN defense plan.
 - Inspect and assess the installation CBRN readiness and preparedness.
 - Execute applicable MOAs or MOUs with activities that will provide mutual aid.
- b. Installation commanders in a foreign operational environment include the following additional requirements:
- Integrate installation and host nation emergency response capabilities to support the sustainment of installation capabilities and readiness.
 - Coordinate installation CBRN defense measures with the respective area or base cluster commanders, if applicable.
 - Identify interoperability requirements and mitigation measures to help meet emergency response requirements.
 - Monitor or support negotiations and/or implementing MOUs and/or MOAs with host nations (HNs), as necessary, to support HN CBRN defense and emergency response assistance.
 - Coordinate training opportunities with supporting HN resources that will periodically exercise existing MOUs and/or MOAs.
 - Review and approve exercise scenarios for CBRN exercises that are consistent with the regional threat assessment.
- c. The responsibilities of the installation staff include:
- Develop, implement, and supervise the organizational CBRN defense program.
 - Coordinate with the appropriate command intelligence section(s) to provide a continuous CBRN threat assessment.
 - Conduct CBRN vulnerability assessment.
 - Develop, coordinate and assess CBRN defense training execution.
 - Integrating installation CBRN emergency response initiatives into installation resource planning.
 - Coordinate with local authorities to ensure that the installation CBRN emergency response plan is integrated with local emergency response plans.
 - Identify roles for tenant and transient units.
 - Ensure that point, standoff, and medical CBRN reconnaissance and surveillance assets support the common operational picture.
 - Coordinate with supporting medical and non-medical laboratory(s) for sample analysis.
 - Conduct inspections to determine the current status of the installation's capabilities, to include strengths and weaknesses in the installation CBRN defense program.

- Conduct periodic reviews of the installation CBRN defense program for improvement and to ensure compliance with the standards.

3. Operational Environment Assessment

a. Threat Assessment. CBRN hazards can range from adversarial actions to man-made incidents/accidents to natural disasters. A key component of the threat assessment requires determining whether a deliberate adversarial capability exists. Many of the hazards however, may originate from technological or natural CBRN disasters. For information on the characteristics of CB agents see *Potential Military Chemical/Biological Agents and Compounds*. For information on radioactive materials of military significance and their effects, see *Multiservice Tactics, Techniques, and Procedures for CBRN Contamination Avoidance*. For information on TIM, see the Emergency Response Guide (current edition).

(1) Assess Adversarial Capability. The installation staff examines available intelligence on potential CBRN hazards, weapons systems, storage facilities, production facilities, research and development programs, and delivery methods. Upon assessing capability, an installation can also conduct direct observation to obtain information on the industrialization in their AO, or from intelligence on other hazards within the area of interest. For example, a vast array of TIM facilities may exist in the AO or near the AO. Further, assessment of an adversary's capability involves several factors that require more specifics, and may generate an intelligence collection plan. Risk is measured when conducting assessments of the possibility of third-power intervention with CBRN weapons on the behalf of an adversary, or the weaponization of a chemical, biological, or radiological (CBR) weapon could occur on a very rudimentary basis with an improvised dissemination device (e.g., handheld spray devices).

(a) Assess Adversarial Opportunity. The installation assesses factors such as when, where, and how an adversary may use a CBRN or TIM weapon or agent. Planners consider the weather, the terrain, the installation boundaries, the defensive posture, and other factors to assess when or where an adversary may attack. Assessment of how an adversary will attack considers the objective (e.g., attacks against critical infrastructure) and subjective factors (e.g., an adversary could attack with no other purpose than to prove his capability or to cause terror). Further, an adversary may attack using overt systems (such as aircraft, cruise missiles, unmanned aircraft systems/remotely piloted vehicles, tactical ballistic missiles and small boats) against operational-level targets. However, covert releases, including various aerosol-releasing devices, contamination of drinking water, radiological dispersal devices (RDD), or improvised explosive devices (IEDs) with CBR components.

(b) Assess Adversarial Intent. Installations conduct an assessment of an adversary's intent to use CBRN weapons or TIM. The adversary's intent may be to cause casualties, contamination, degradation or panic or demonstrate its ability to attack anywhere at anytime.

(2) Technological and Natural CBRN Disasters. Major accidents and natural disasters occur on a continuing basis and may involve CBRN agents/materials. Consequently, CBRN defense plans need to address avoidance, protection, and decontamination functions within an installation's AO, and across the area of interest.

(3) **Assess Impact.** Planners assess the impact of a CBRN or TIM attack or incident on the installation. Attack templates identify whether the attack is conducted on or off the installation. For example, attack scenarios could include point source attack on an installation or line source attacks upwind of the target. The source of the attack assessment may occur at the installation level using decision support tools (DSTs) or by exercising technical reach-back.

(4) **Assess the Operational Environment.** The operational environment may be a permissive, uncertain, or hostile environment. As a permissive environment, the military and/or law enforcement agencies (LEAs) should have control and the intent and capability to assist operations. An uncertain operational environment could be one in which the host government forces, whether opposed to or receptive to operations, do not have effective control of the territory and population in the intended AO. A hostile environment includes adversarial forces that have a degree of control, the intent, and the capability to effectively oppose or react to operations.

(5) **Assess Previous Incidents/Past Use.** The installation planner must think “outside of the box.” The planner collects information on previous uses of CBRN agents or weapons, and also obtains information on TIM incidents or accidents that may have occurred in the AO. The planner’s assessment also considers how an installation may be affected by TIM release (as a secondary hazard from a naturally occurring incident such as hurricanes or floods). As assessments on previous use of TIM are conducted, hazards may occur based on the manufacture, storage, distribution, or transport of those materials in close proximity to installations. Deliberate or inadvertent release significantly increases hazards to the indigenous population and U.S. forces. Given the prevalence of TIM throughout the world, civilian and DOD planners use area studies and integrate intelligence estimates to assess possible TIM hazards. TIM should be recognized for the singular hazards they pose and the potential risks that may result from an explosion or a fire. Some representative sources of TIM hazards are shown in Table II-1.

Table II-1. Potential TIM Hazard Sources

- | |
|--|
| <ul style="list-style-type: none">• Agricultural—includes insecticides, herbicides, and fertilizers.• Industrial—chemical and radiological materials used in the manufacturing processes, fuel, or in cleaning.• Production and research—CB materials produced or stored in a facility.• Radiological—nuclear power plants, medical facilities, and laboratories nondestructive testing facilities and food/mail irradiator facilities. |
|--|

(6) **CBRN Threat Levels.** CBRN threat levels serve as a marker for establishing the level of CBRN threat posed by an adversary. CBRN threat levels should be in accordance with Standardization Agreement (STANAG) 2984. Table II-2 provides an overview of the CBRN threat levels.

Table II-2. CBRN Threat Levels

CBRN Threat Level	Description
Zero	The belligerents have no known offensive CBRN capability.
Low	The belligerents have an offensive CBRN capability, but there is no indication of its use in the immediate future.
Medium	Nuclear, biological, or chemical weapons have been used in another AO or there are strong indications that the belligerents will use these weapons in the immediate future.
High	Nuclear, biological, or chemical attack is imminent.

b. Physical Environment.

(1) The physical environment includes terrain, weather, and the commander's geographic framework. Terrain and weather effects must be continuously assessed so that decision support tools and predictive modeling capabilities are integrated with environmental conditions.

(2) Installation Zoning and Split-MOPP. An installation commander may elect to establish zones for the installation to provide flexibility and maximize mission performance in the event that a CBRN incident occurs. Further MOPP analysis may be expanded to include split-MOPP operations within the established installation protection zones at installations where MOPP is the personnel protection level employed. Appendix F provides more detail on establishing zones and integrating split-MOPP for an installation CBRN defense plan. Some installation zoning principles are shown in Table II-3.

Table II-3. Installation Zoning Principles

<ul style="list-style-type: none">• Consider the location of key functions (e.g., work centers) within different zone sectors.<ul style="list-style-type: none">○ A very large zone may be practical if only a few functions are located in the area.○ One large work area with a clearly defined boundary is a good candidate for a zone.• Consider physical features.<ul style="list-style-type: none">○ Zone boundaries should be clearly identifiable.○ Group similar surface areas into the zone.• Consider the terrain. If part of an installation has a significantly higher elevation, consider aligning a zone boundary along an identifiable contour interval.• Consider accessibility (such as the presence of clear access routes).• Consider responsibility assignments for the area.• Consider the consistency with ground defense sectors. The CBRN zones should be the same as the ground defense sectors.

c. Information Environment. The installation commander and staff maintain constant situational awareness and updates to the common operational picture. Intelligence assessments must be integrated between military and civil sources. The commander must consider requirements and existing agreements for information sharing among the civil-military stakeholders. Assumptions may be required, but the plan must call for means by which to confirm or deny these assumptions through information collection efforts. In addition, the information environment may include predictive modeling, meteorological data, data from an integrated detection network, and readiness reporting.

d. Political Environment.

(1) **Jurisdictional Authority.** The installation commander must establish the level of authority in exercising military operations on or off the installation. This level of authority will conform to public law, local agreements, or military regulations and standards. Assessment of the political environment must include the level(s) of authority that the military commander may exercise when implementing the installation CBRN defense plan. One example of this includes the appropriate level of personal protection equipment required by CBRN responders. Operations in support of civil authorities may be subject to public law or host nation agreements, where contingency operations may give the commander more flexibility to apply risk management and subsequently lower the level of protection.

(2) **Agreements.** Installations range in size and complexity. Small or simple installations may not have organic emergency response resources of large or complex ones. The installation commander evaluates essential functions during the development of the CBRN defense plan. The national response plan (NRP) provides a list of emergency support functions (ESFs) that the installation commander may implement – or may be required to implement – into the overall CBRN defense plan. Appendix B provides the details for the 15 ESFs from the NRP. The commander assesses the requirement and then determines if he has the requisite capability. Capability shortfalls may be overcome by agreements with civil authority capabilities. Inversely, the commander may be required to support civil authorities by providing capabilities to fill gaps that are identified for civil response.

(3) The Domestic Environment.

(a) **National Incident Management System (NIMS).** The national structure for incident management establishes a clear progression of coordination and communication from the local level to regional and national HQ levels. For the military installation, use of NIMS supports the interoperability between installations and with the civilian community. Use of NIMS is an important interoperability tool for the different service components that will operate together on an installation. Chapter IV discusses the implementation of the NIMS with respect to the ICS. The NIMS process supports the following:

- Integrating incident-related prevention, mitigation, response, and recovery activities.
- Improving the coordination and integration within the military AO and with federal, state, local private-sector, and nongovernmental organization (NGO) partners.
- Increasing the efficient use of resources needed for more effective incident management.
- Improving situational awareness (SA) within the installation.
- Facilitating requests for assistance (RFAs) for support that exceeds an installation's response capability.
- Providing linkage to technical reach-back capabilities.

(b) **National Response Plan (NRP).** The NRP is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. Because the purpose of the NRP is to establish a comprehensive, national, all-hazards approach to domestic incident management, most installation response plans must be consistent with the guidance found in the NRP. The services or combatant commands should consider standardized procedures and provide a common emergency planning template that would also facilitate interoperability among the different components serving on an installation.

(c) **Title 10 USC Support.** Installation title 10 USC assets may receive tasks to provide support to validated RFAs. Installation resources capable of providing the necessary response are then sent to the incident area, normally OPCON to the Defense Coordinating Officer (DCO) or JTF (during a CBRN incident), to perform the tasks. National Guard (NG) units may be mobilized and employed under installation 10 USC units; however, they will be subject to employment according to applicable command or support relationships established by the governing headquarters (such as COCOM or OPCON).

(d) **Title 32 USC Support.** Installation-based NG units are primarily a state response force. They will normally remain under the control of the governor, through the adjutant general (TAG). In this capacity their missions are conducted under the state emergency management framework. However, installation NG units assigned to an installation could operate (on or off the installation) within its state of assignment or within another state under one of four potential authorities:

- **Immediate Response.** Under DOD Directive (DODD) 3025.1, imminently serious conditions resulting from any civil emergency or attack may require immediate action by military commanders or responsible officials of other DOD agencies to save lives, prevent human suffering, or mitigate great property damage.
- **Interstate Compacts.** Several interstate compacts provide for mutual aid between states for disaster response. These agreements occur between the states; however, the states may provide DOD with information on their interstate agreements. The most comprehensive of these, the Emergency Management Assistance Compact (EMAC), provides habitual relationships that facilitates emergency planning. NG support under EMAC occurs in state active-duty status. Therefore, the EMAC is not applicable to NG units performing their mission exclusively in 32 USC or 10 USC status.
- **State-to-State MOAs.** In an emergency situation, the governor or other appropriate officials, according to state laws, could rapidly develop a simple MOA addressing NG support. This process is commonly used by states that are not EMAC signatories but wish to receive or provide support on a case-by-case basis.
- **Mobilization Under 10 USC.** A reserve component unit could be called to active duty under the mobilization statutes (voluntary mobilization, presidential selective reserve call-up, partial mobilization, or full mobilization) and then be employed as

directed by the President of the United States (POTUS) or his designee (see *Joint Tactics, Techniques, and Procedures for Manpower Mobilization and Demobilization Operations: Reserve Component (RC) Callup* for more detailed information). The decision to mobilize NG units is the responsibility of the POTUS based on a recommendation from the Secretary of Defense (SecDef). If a NG unit is mobilized, the unit will be assigned to the C2 element of the designated, supported combatant commander.

(e) **Regulatory and Legal Considerations.** Military units supporting an installation emergency response will always be under the C2 of military authorities, yet they may work in support of the civil authorities assisting the installation. The legal considerations for CBRN response on an installation are complex, varying by the location, the area affected, and the type of incident. Commanders should consult their legal staff at the beginning of the planning process to incorporate, understand, and train staffs and responders on the limitations that a particular installation might face. Commanders, in conjunction with their judge advocate general (JAG), should assess the preparedness of the legal staff and ensure the legal staff receives appropriate training to deal with terrorist CBRN attacks. Representative legal planning considerations that influence response activities include some of the following considerations:

- The use of chemical and biological weapons within the US is a federal offense under 18 USC Section 175 (biological weapons possession); and Section 229 (CB weapons use as a WMD).
- The commander's inherent authority to maintain law and order on a military installation coupled with the mandatory responsibility to protect personnel, facilities, and material also guides response to a prewar incident in the United States, its territories or possessions, the District of Columbia, and other places subject to U.S. jurisdiction. In these cases, the Federal Bureau of Investigation (FBI) has investigative jurisdiction and should be immediately notified when an incident occurs. Incident/attack locations should be treated as crime scenes, insofar as reasonably possible, and the normal chain of custody procedures should be followed for any item that is removed from the incident scene. These authorities, responsibilities, and actions are according to DODD 5525.5 and implemented by AR 500-51.
- Should the effects of an installation terrorist CBRN incident or attack extend to surrounding civilian communities; or when the need to save lives, prevent human suffering, or mitigate great property damage caused by an off-installation event, the installation may respond immediately, if requested. The responding commander will report to higher HQ as soon as possible following the initiation of the response effort.
- Requests for an immediate response (i.e., any form of immediate action taken by a DoD Component or military commander to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions) may be made to any

Component or Command. The DoD Components that receive verbal requests from civil authorities for support in an emergency may initiate informal planning and, if required, immediately respond as authorized in DoD Directive 3025.1. Civil authorities shall be informed that verbal requests for support in an emergency must be followed by a written request. (according to DODD 3025.15).

(4) The Foreign Environment.

(a) Host Nation (HN) Agreements and Treaties. During peace operations, HN agreements and treaties may direct U.S. forces to provide assistance during CBRN events. In these instances, installation assets may receive taskings to provide support to a HN response. U.S. forces will remain under U.S. command.

(b) Status of Forces Agreement (SOFA). A SOFA between the United States Government and a HN generally governs the authorized activities of U.S. personnel and the installation. Most SOFAs, such as North Atlantic Treaty Organization (NATO) SOFA Article VII, paragraph 10, and Japan SOFA Article XVII, paragraph 10, state that the U.S. has the right to police and maintain order on the premises it occupies. Most SOFAs require U.S. military authorities to assist the HN with incident investigation and turn over all evidence to the HN authorities when requested. Commanders must also identify legal authorities and requirements before conducting joint training exercises with HN elements.

(c) Sovereignty Issues. During peace operations, U.S. forces must be aware that HN laws may require the sharing of information, to include samples of CBRN agents during a CBRN event. The release of information or material is likely a strategic or operational-level war issue, and the installation commander will respond according to the command guidance furnished.

(d) Stability Operations. HN agreements and treaties and SOFA will likely remain in affect during contingency operations in countries where U.S. forces are based and operate, unless the agreement or treaty is with a country in which the contingency operations are directed. In this case, the United States will determine its responsibilities under U.S. and international laws. During contingency operations, issues of sovereignty during a CBRN event will be addressed by applicable contingency plans, orders, and rules of engagement.

4. Vulnerability Assessment

a. Developing the installation CBRN defense plan requires comparison of the threat with installation vulnerabilities in order to determine efforts to mitigate CBRN effects before an incident occurs. Vulnerability assessment also includes integration of commander's guidance through a risk management process in order to prioritize vulnerability reduction measure implementation. Vulnerability assessment during the planning phase begins with the identification of the hazards and an analysis of each (see Figure II-2). Vulnerability assessment during the planning phase continues by integrating the specific threat assessment with analysis of specific vulnerabilities and identification of potential vulnerability reduction measures. The endstate during the planning phase is typically a staff estimate (running estimate for U.S. Army) and recommendation to the commander on the priorities for vulnerability reduction. The

commander must provide risk management guidance that determines which vulnerability reduction measures to implement, and which to abandon or postpone. The assessment is an appraisal of the strengths and weaknesses of the installation functions as compared to the threat. Chapter III provides additional detail for the completion of the vulnerability assessment process.

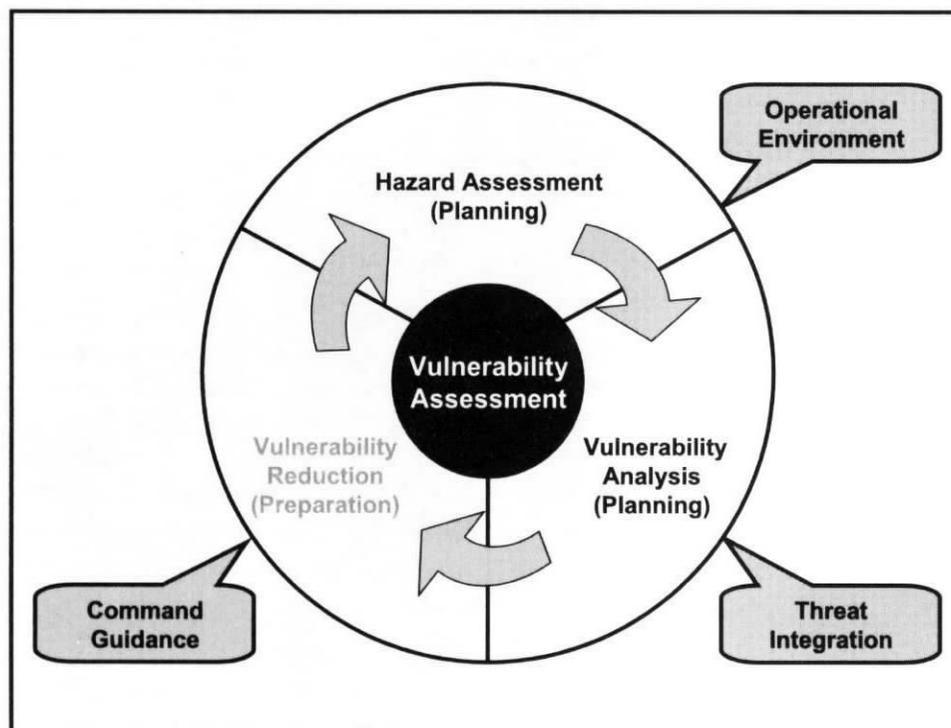


Figure II-2. Vulnerability Assessment During the Planning Phase

b. Analyzing key assets and critical infrastructure should be conducted during the CBRN VA, when possible. Automated tools at the installation or available via technical reach-back capability can be used to perform the following functions:

- Conduct a blast effects analysis from explosive munitions and devices.
- Conduct a weapons effects analysis from CBRN and/or TIM.
- Conduct the analyses and plot the effects on a map or image to identify the key assets and critical infrastructure (e.g., people, structures, equipment) that could be affected by a CBRN or TIM event. If possible, include the projected fatalities, contamination, casualties and impact on installation readiness.
- Coordinate with and provide results of the analyses to the commander and his staff.
- Use the results to help produce courses of action during the estimation process.

c. An accurate CBRN VA is the groundwork for the strategy. The strategy is used to develop and execute vulnerability reduction measures. The *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear*

Vulnerability Assessment provides further guidance for conducting a CBRN VA and developing CBRN vulnerability reduction measures.

5. Commander's Guidance

Commander's guidance includes the vision, intent, key tasks, mission, priorities, and overall strategy – to include acceptable risk.

a. The commander and staff develop a vision and corresponding strategy that defines successful installation readiness and preparedness by balancing threat, vulnerability, and risk. This guidance gives definition to the installation's mission, the commander's intent, and the goal of the installation CBRN defense program. It orients on the future and provides a clear, concise statement of the precise picture of installation readiness and preparedness. It could include comments about healthy relationships with the local community or effective security measures to deter a prospective terrorist from using CBRN weapons. In short, the vision gives the commander's view of the end product of the installation's CBRN readiness and preparedness. The vision includes identified key tasks or critical functions that support the installation's ability to accomplish its assigned mission. It also takes into account the inherent responsibility to protect people and property.

b. **Strategy Development.** Using assessments as the starting point and the vision as the end point, the commander and staff develop the CBRN defense strategy. The strategy provides the method by which installation CBRN readiness and preparedness will be achieved. The strategy is the road map for building an installation CBRN defense program over a period of time. The strategy should—

- Focus on the threat.
- Identify the phases or steps to reach the vision.
- Assign objectives and vulnerability reduction measures to each phase.
- Identify the main and supporting vulnerability reduction measures in each phase.
- Assign priorities for resources in each phase.
- Identify indicators of success to monitor the progress of the strategy.
- Assess readiness to respond to CBRN events.

6. Plan Development

a. **Military Decision Making Process (MDMP).**

(1) The responsibility for CBRN defense decisions, plans, and supervision rests on the commander. For many years, commanders have used a planning process known as the military decision making process (MDMP) to determine the best course of action (COA) to be written into a plan. Figure II-3, provides an overview of this process.

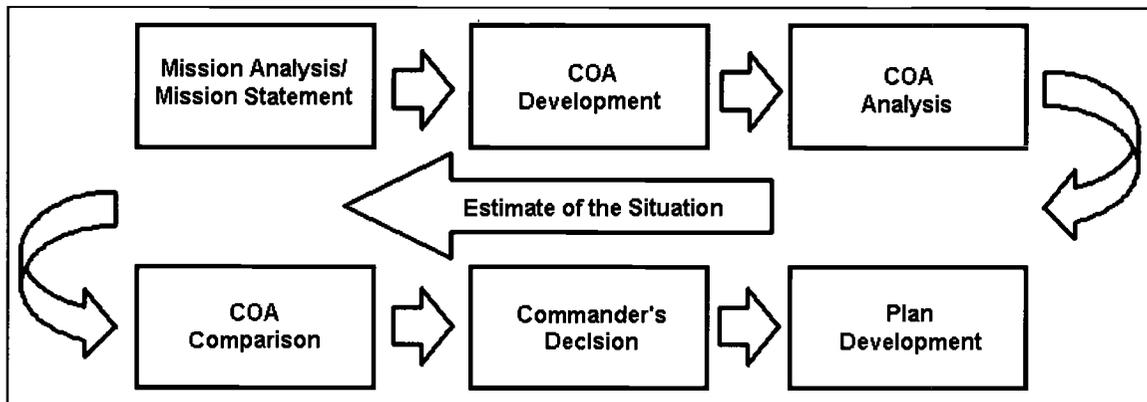


Figure II-3. Military Decision-Making Process

(2) The process provides a framework for determining a plan of action for emergency response. The installation uses these process steps to develop an effective solution to the challenge of preparing a viable and comprehensive emergency management plan. The estimate process is used by each service component and provides a common framework for an installation that may have components from the different services.

(3) Once the COAs have been developed and analyzed, the commander compares and considers multiple COAs that support the installation CBRN defense mission. In a CBRN plan, the recommended COA encompasses preparation, response, and recovery phases. Variables will include modifications to the plan dependent on type of CBRN or TIM hazard involved in the incident. For example, the COA that outlines the response to a biological or radiological attack may differ from the COA for a chemical attack.

(4) Installation CBRN defense plans are living documents. The installation CBRN defense plan should be planned, staffed, exercised, and approved by the installation commander. Once approved, the installation CBRN defense program transitions from the planning to the preparation phase. As preparation proceeds, assessments are continuously updated and may require re-visiting and revising the installation CBRN defense plan. Chapter III discusses the installation CBRN defense preparation phase in more detail.

b. Resource Allocation and Prioritization. As part of the development of the CBRN defense plan, resources identified by the installation are allocated to prioritized requirements. The prioritization is made by the commander with input from his staff.

c. Key Elements of the Plan. The plan should address each ESF role and how they are integrated and synchronized with respect to response and recovery.

(1) C2. The installation CBRN defense plan is aligned with the installation C2 architecture. The use of ICS, or tactical equivalent, provides a means of maintaining SA during CBRN incident responses.

(2) Functional Organization. An example of the management organization used by ICS is discussed in Chapter IV. This organization is mandated by the NIMS, but provides a potential model for commander's operating tactical or expeditionary bases for which the NIMS is not required.

(3) **Organization by ESF.** Appendix B describes the ESFs, and Chapter IV discusses a method of organization response measures that relates the functional components of the ICS to the ESFs as a method by which to ensure that the plan accounts for these critical tasks. The installation commander may have a complex staff to incorporate this functional organization, or may assign multiple functions to singular staff elements.

This page intentionally left blank.

is presented in a logical order for preparing and improving an installation's CBRN defenses:

- Acquisition of necessary CBRN defense equipment.
- Preparation of facilities.
- Education and training.
- Coordination, monitoring, and reporting requirements.
- Conducting response exercises.
- Reassessing capabilities and identifying remaining vulnerabilities.

2. Acquisition of Necessary CBRN Defense Equipment

a. **Specialized CBRN Defense Equipment.** The nature of CBRN agents is such that highly specialized equipment is necessary to detect and defend against attacks involving weapons containing these substances. The use of CBRN sensors, detectors, surveillance, and alarms is therefore a vital part of the defense strategy in preparing an installation CBRN defense plan. The first step to properly preparing an installation against a possible CBRN attack is the acquisition, installation, and employment of this specialized equipment necessary for effective detection and defense against such an attack. DOD has recently instituted a "tiered approach" to installation CBRN defense. This approach, using a graduated scale of employment based on priority, was designed to be flexible enough to accommodate the needs of specific installations while standardizing major system elements to provide cost effective solutions. Appendix J provides further details about this DOD tiered program for manning, training, and equipping the response force for CBRN defense.

b. **JPM Guardian.** On May 6, 2003, the Joint Project Manager-Guardian (JPM-Guardian) was formally established "to provide Department of Defense (DoD) prioritized installations with an integrated chemical, biological, radiological, nuclear (CBRN) protection and response capability to reduce casualties, maintain critical operations, contain contamination and effectively restore critical operations". JPM-Guardian was established to "provide an effective CBRN protection, detection, identification and warning system for installation protection, ensure integration of CBRN network with existing Command, Control, Communications, Intelligence (C3I) capabilities to provide effective information management, provide a capability that will allow for rapid restoration of critical installation operations, protect DoD civilians, contractors and other persons working or living on U.S. Military installations and facilities, and equip and support Coalition Support Teams, Installation Support Teams, Regional Response Teams and recon/decon teams." JPM Guardian should be contacted for guidance on what specific equipment should be installed on a particular DOD installation.

c. **CBRN Detection and Surveillance.** The TTPs outlined in the Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Reconnaissance and Multiservice Tactics, Techniques, and Procedures for Biological Surveillance provide guidance on establishing installation CBRN detection and

surveillance arrays. The operational use of the detector arrays should be linked to the CBRN threat level. As the CBRN threat level increases, CBRN detection and surveillance operations should also increase, as follows:

- (1) At CBRN Threat Level Zero, the IC and staff may choose not to activate or emplace CBRN detection and surveillance devices.
- (2) At CBRN Threat Level Low, an IC and staff may choose to position detection and surveillance devices as appropriate but not activate them.
- (3) At CBRN Threat Level Medium, an installation could operate detection and surveillance devices on a periodic basis when conditions were favorable for a CBRN attack. For example, an available JBPDS could be run in early evening, when conditions were favorable for a biological attack.
- (4) At CBRN Threat Level High, all available CBRN detection and surveillance devices appropriate for the threat could be operated. Care must be taken to insure power supplies and expendables are available for such operations. An installation CBRN detector array is only one source of information that supports the installation common operational picture (COP). Other critical information input (such as medical surveillance [MEDSURV], individual reports of unusual activity, or individuals experiencing chemical agent symptoms) also contributes to the installation CBRN SA.

3. Preparation of Facilities

a. **Critical Facilities.** Facilities identified as 'critical' in the installation's emergency response plan are integrated into the CBRN defense plan. Installation activities improve installation preparedness by fortifying shelters, protecting vital equipment (e.g., covers, sheltering), and improving or preparing individual fighting positions. These actions and prior planning can protect against conventional and some CBRN weapons effects.

b. **Special CBRN Defense Measures.** Specific CBRN-defensive measures needed to protect facilities are identified in the VA process. See the Multiservice Tactics, Techniques, and Procedures for CBRN Contamination Avoidance and the Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Protection for additional information on measures that can be taken for the preparation of facilities. Representative measures that can be taken include the following:

- (1) Provide safeguards in and around building HVAC systems to minimize the possibility of a covert CBRN attack.
- (2) Identify alternate sources of electricity or water for key facilities
- (3) Identify alternate facilities to house key functions should the primary facility become uninhabitable.

- (4) Verify the serviceability of facility collective protection (COLPRO).
- (5) Prepare SIP kits for buildings that may not have COLPRO.
- (6) Identify shelter management personnel and provide provisions for shelter locations.
- (7) Provide effective communications to facility occupants.

4. Education and Training

a. Education. Installation incident management organizations and personnel at all levels must be appropriately educated to effectively provide the installation with an all-hazards incident management capability. CBRN incident response operations need to be adequately emphasized in applicable programs of instruction. For those units without experience in civilian exercises on a local, state, regional, or national basis, limited opportunities exist to incorporate lessons learned from these events into the training environment such as institutional education, simulations, and exercises. All personnel should be educated in basic CBRN awareness and personnel assigned special responsibilities receive more specific operational instruction. Numerous courses and training opportunities are available from various government and private sources. A compendium of these resources is available from FEMA. Some of the educational opportunities available are in the following areas:

- (1) General Awareness.

- (a) Force Protection (FP)/Anti-Terrorism (AT). One component of combating terrorism includes defensive measures against terrorist attacks. All personnel train on the fundamentals necessary to defend installations, units, and individuals against terrorist attacks. AT is a FP measure and is the responsibility of commanders at every level.

- (b) Overview of CBRN Counter-Terrorism (CT) Operations. Based on the roles and responsibilities of the audience, this may include the fundamentals of the NRP, the ICS, and service-specific issues.

- (2) Specific Operational Education for Command and Staff.

- The role of the action agency and Lead Federal Agencies (LFAs).
- Legal authorities, constraints, and limitations.
- Logistics and support requirements, including fiscal reimbursement issues.
- C2 structures.

NOTE: An example of this type of training is the DOD Emergency Preparedness Course. This course prepares Emergency Preparedness Liaison Officers (EPLOs), and staffs to plan and execute joint military operations that support civil authorities responding to domestic emergencies and disasters. The US Forces Command offers the course eight times a year at the FEMA Mount Weather Emergency Assistance Center, Berryville, Virginia, and conducts mobile training teams within the USPACOM's and the US Southern Command's AORs each year. This training is authorized by DODD 3025.1.

b. Training. Installations must train to perform individual and collective CBRN defense tasks as units and joint forces. Licensing and certification standards vary based on geographical location and equipment available on the installation. Commanders should ensure that all operators are fully trained to complete their assigned missions. Training must be provided to HN military and civilian work forces and US contractors on the installation.

(1) Training Tasks. The installation conducts training on key UJTL and applicable service training tasks that support preparedness, response and recovery measures. Using the UJTL as a baseline helps to support a common framework for training.

(2) Training Conditions. The installation uses a simulated CBRN or TIM environment as a condition for selected training events. The degradation experienced by operating in the appropriate protective posture improves installation preparedness. This type of training provides installation leadership with an assessment of the effectiveness of vulnerability reduction measures.

(3) General Installation Training Considerations. CBRN awareness training is available for every military service member, DOD civilian, contractor, appropriate family member, and local national hired by the DOD—regardless of rank. These personnel should be aware of CBRN actions and effects, the need to maintain vigilance for possible CBRN actions, and methods for employment of CBRN TTP. To ensure an effective response, an installation-wide, cross-functional training program should be implemented. Thorough training is required to prepare individuals and emergency teams to safely and efficiently respond to a terrorist CBRN attack at their required level of proficiency.

(4) Incident Management Training.

(a) General Considerations. Installations must have personnel trained to respond to a CBRN attack. All persons participating in the response to CBRN incidents should be trained to competently perform within the incident command system (ICS)/unified command (UC) structure.

(b) Minimum Requirements. The following are minimum requirements for installation incident management personnel:

(b) **Minimum Requirements.** The following are minimum requirements for installation incident management personnel:

- Entry level first responders (including firefighters, police officers, emergency medical services providers, public works on-scene personnel, public health on-scene personnel and other emergency responders) and other emergency personnel will require an introduction to the basic components of the Incident Command System. (FEMA IS-700: NIMS, An Introduction ICS-100: Introduction to ICS or equivalent)
- First line supervisors, single resource leaders, lead dispatchers, field supervisors, company officers and entry level positions (trainees) on Incident Management Teams and other emergency personnel will require a higher level of Incident Command System training. (IS-700, ICS-100 and ICS-200: Basic ICS or its equivalent)
- Middle management, strike team leaders, task force leaders, unit leaders, division/group supervisors, branch directors and Multi-Agency Coordination System/Emergency Operations Center staff require higher level Incident Command System training. (IS-700, IS-800 NRP, ICS-100, ICS-200 and in FY07, ICS-300)
- Command and general staff, agency administrators, department heads, emergency managers, area commanders and Multi-Agency Coordination System/Emergency Operations Center managers also require higher level Incident Command System training. (IS-700, IS-800, ICS-100, ICS-200 and in FY07, ICS-300 and ICS-400)
- All personnel providing support to civil authorities must be knowledgeable of the NRP prior to providing support by completing the DHS, FEMA, Emergency Management Institute IS-800 course "National Response Plan and Introduction".

(5) **First Responder Training.**

(a) **General Considerations.**

- All local responding personnel must be trained at least to the first responder operations level.
- Persons functioning in more complex roles, such as IC, HAZMAT team leader, or technician, must have completed

additional training appropriate for the functions to be performed.

- Training competencies for each of these roles and functions are fully defined in the above standards and regulations.
- The competency and training requirements for local responders and technical experts are defined in 29 CFR 1910.120, the Occupational Safety and Health Administration (OSHA), National Fire Protection Association (NFPA) Standards 471, 472, and 473, and in reference resources, such as Department of Transportation (DOT)/Federal Emergency Management Agency (FEMA) Guidelines for Public Sector Hazardous Materials Training.
- Requirements for all roles include training necessary to perform correctly within the ICS/UC structure at an incident.

(b) **Specific Requirements.** Personnel who participate, or are expected to participate, in emergency response shall complete the following training:

- First responder awareness-level training is for personnel who are likely to witness or discover an incident, and who have been trained to initiate an emergency response sequence. This training should be provided for all installation personnel. These personnel would take no further action beyond notifying the authorities of the hazard.
- First responder operations-level training is required of personnel who respond to incidents as part of the initial response to the site for the purpose of protecting persons, property, or the environment from effects of the hazard. This includes security guards, military police, incident response team members, emergency medical personnel, and firefighters. These personnel are trained to respond in a defensive fashion without actually trying to contain the hazard. They are required to receive at least eight hours of training and to demonstrate competency.
- HAZMAT technician-level training is provided for personnel who respond for the purpose of containing the hazard. This training is required for HAZMAT team members. They are required to receive at least 24 hours of training equal to responder operations-level training and to demonstrate additional competencies.

- HAZMAT specialist-level training should be provided for incident response team specialists who respond with and provide support to HAZMAT technicians. However, their duties require more specific knowledge of the various substances to be contained. These personnel also act as site liaison with other authorities regarding site activities. They are required to receive at least 24 hours of training equal to responder technician-level training and to demonstrate additional competencies.
- On-scene IC-level training is provided to those who are to assume control of the incident scene. They are required to receive at least 24 hours of training equal to responder operations-level training and to demonstrate additional competencies.

c. **Training Evaluations.**

(1) Evaluations can be either internal or external. Internal evaluations are conducted at all levels and are implemented into all training. External evaluations are usually more formal and are conducted by the next higher HQ.

(2) A critical weakness in training is the failure to evaluate each task every time it is executed. The exercise evaluation concept is based on simultaneous training and evaluation. Every training exercise provides the potential for evaluation feedback. Every evaluation is a training session. For the program to work, trainers and leaders must continually evaluate training as it is executed.

(3) External evaluations are administered at the discretion of the chain of command and are conducted to evaluate the ability to perform its critical response missions.

5. Coordination, Monitoring, and Reporting Requirements

a. **Coordination.**

(1) **Who Needs to Coordinate?** One major objective of preparedness efforts is to ensure mission integration and interoperability in response to emergent crises across functional and organizational lines, as well as between public and private organizations. Each installation must therefore make certain that the CBRN response plans of the various components, agencies and sections within that installation have been thoroughly coordinated with each other as well as with the response plans of tenant units, the plans of local, state, and federal organizations, and the plans of any Joint Task Forces, Coalition Forces or Host Nations (HN). These organizations represent a wide variety of resources, and representatives from each entity / capability should meet regularly to coordinate.

(2) **Focus of Coordination Efforts.** These installation, local and regional CBRN defense experts should meet to ensure that proper consideration has been placed on planning (identify threats, determine vulnerabilities, and identify required resources), training and exercises, personnel qualification and certification, equipment certification, and other preparedness requirements within and between installations and surrounding resources (civil or HN). Another focus should be to identify the range of deliberate and critical tasks and activities necessary to build, sustain, and improve the operational capability of the installation to prevent, protect against, respond to, and recover from any CBRN incident. The needs of the installation involved will dictate how frequently such coordination efforts should occur as well as how they are structured.

(3) **Mutual-Aid Agreements (MAA).** Mutual-aid agreements are the means for installations and local, state Federal, (HN or any other outside organization) to provide resources, facilities, services, and other required support to one another during an incident. Each installation should be party to a mutual-aid agreement (such as the Emergency Management Assistance Compact) with appropriate agencies (units/organizations) from which they expect to receive or to which they expect to provide assistance during an incident. This would normally include all neighboring or nearby organizations, as well as relevant private-sector and nongovernmental organizations. Mutual-aid agreements are also needed with private organizations, such as the American Red Cross, to facilitate the timely delivery of private assistance at the appropriate organizational level during incidents. At a minimum, mutual-aid agreements should include the following elements or provisions:

- (a) Definitions of key terms used in the agreement.
- (b) Roles and responsibilities of individual parties.
- (c) Procedures for requesting and providing assistance.
- (d) Procedures, authorities, and rules for payment, reimbursement, and allocation of costs.
- (e) Notification procedures.
- (f) Protocols for interoperable communications.
- (g) Relationships with other agreements among organizations.
- (h) Workers compensation.
- (i) Treatment of liability and immunity.
- (h) Recognition of qualifications and certifications.
- (i) Sharing agreements, as required.

NOTE: More information and examples of MAAs can be found at Web site <http://www.nimsonline.com/download_center/index.htm#mutual>

b. **Monitoring.** Any analysis of an installation's CBRN defense status should include a step-by-step review of command SOPs and associated formal checklists from the functional elements on the installation (e.g., HAZMAT, law enforcement, fire, and emergency medical services). As was mentioned previously, these emergency response checklists should be analyzed to insure that maximum coordination between responding elements exists in each SOP.

c. **Status Reporting.** Each installation activity (including tenant units) responsible for different aspects of the CBRN defense plan (e.g., HAZMAT, law enforcement) should be tasked to periodically report their operational status to the installation operations center. This status reporting helps to ensure that the installation CBRN defense plan is updated, executable, and relevant.

6. Conducting Response Exercises

a. **General Considerations.** Education and training are not enough to prepare an installation. The use of realistic exercises is required to ensure that the installation can conduct operations under CBRN or TIM conditions. Aspects to consider when developing an exercise should include the following:

(1) Exercises should include participants from all emergency response functions on the installation and whenever possible, appropriate local, State, Federal, and host-nation participants.

(2) Each exercise should include realistic CBRN and TIM scenarios that the installation could face based on the current threat assessment.

(3) When appropriate, OCONUS installations should align their installation exercise and training schedule with the Combatant Commanders, host-nation, and the Department of State-related CBRN exercises.

(4) Each exercise should provide realistic master events sequence lists that exercise each element of the installation emergency response plan. Unexpected challenges (e.g., disabling key personnel and equipment) are included to assess the resiliency of the response process.

(5) HN civilians supporting installation operations may require frequent rehearsals and refresher training.

(6) Tabletop exercises can be used to provide the installation leadership and staff with opportunities to war-game multiple scenarios. Tabletop training exercises are specifically designed to train the leaders to execute the critical missions and critical collective tasks.

(7) When possible, installations should consider aligning their installation exercise and training schedules with that of the Department of Justice, the Office of Domestic Preparedness exercise and training programs as well as State and local preparedness programs to include WMD CSTs, as appropriate.

b. **Exercise Design.** Each exercise should be designed to evaluate specific critical missions or tasks within the overall evaluation scenario. Evaluators should make every effort to support the evaluation. By the same token, serious thought should be given to those conditions that obstruct an accurate assessment of the unit's performance. The evaluators must know the test thoroughly and precisely to implement it correctly. The use of realistic exercises is required to ensure that the installation can conduct operations under CBRN or TIM conditions.

c. **Evaluator Knowledge.** Each evaluator, regardless of position, must have expert knowledge of capabilities and responsibilities, communications equipment, weapons, and vehicles, and should thoroughly understand mission. Poor evaluator training may result in poor after-action or lessons-learned information. Note: The following link may be useful in preparing an evaluation staff for evaluating a CBRN exercise: <http://www.training.fema.gov/EMIWeb/downloads/IS139EvalPlan.doc>

d. **Periodicity of Exercises.** Installations should conduct annual CBRN exercises using realistic CBRN scenarios appropriate to the installation's mission and vulnerabilities to validate the concept of operations articulated in their CBRN emergency response plan. Scenarios should consider terrorism, technological accidents, and natural disasters that may result in CBRN releases and incidents. Training exercises are used to train and practice the performance of collective tasks to execute the unit's primary mission and other critical tasks.

7. Reassess Capabilities and Identify Remaining Vulnerabilities

a. The installation CBRN defense vulnerability assessment must be an almost continuous process (see Figure III-2). Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Vulnerability Assessment provides further guidance on the VA cycle. After the installation's CBRN defense plan is implemented, the installation senior staff should start scheduling periodic follow-ups to reassess these CBRN defense preparations. These periodic follow-ups help ensure that necessary resources remain properly deployed, prepared, and synchronized to successfully execute CBRN defense tasks. The timing of these recurring reassessments should not be just based strictly on time (calendar year, etc) however. Other factors such as changes in the threat or changes in unit or resource availability should also be considered when scheduling installation CBRN defense reviews.

b. Pre-incident checks verify that installation personnel and units have supplies and equipment such as the required individual protective equipment (IPE) and COLPRO equipment.

c. The measures that comprise protection actions also provide VA feedback. This feedback improves the overall installation CBRN response plan. For example, US CBRN personnel may take notice of the shortcomings of HN protective equipment (i.e., protective ponchos issued by some nations, which may be effective in protecting against a direct spray hazard but would provide little protection against regional mustard contamination on an installation).

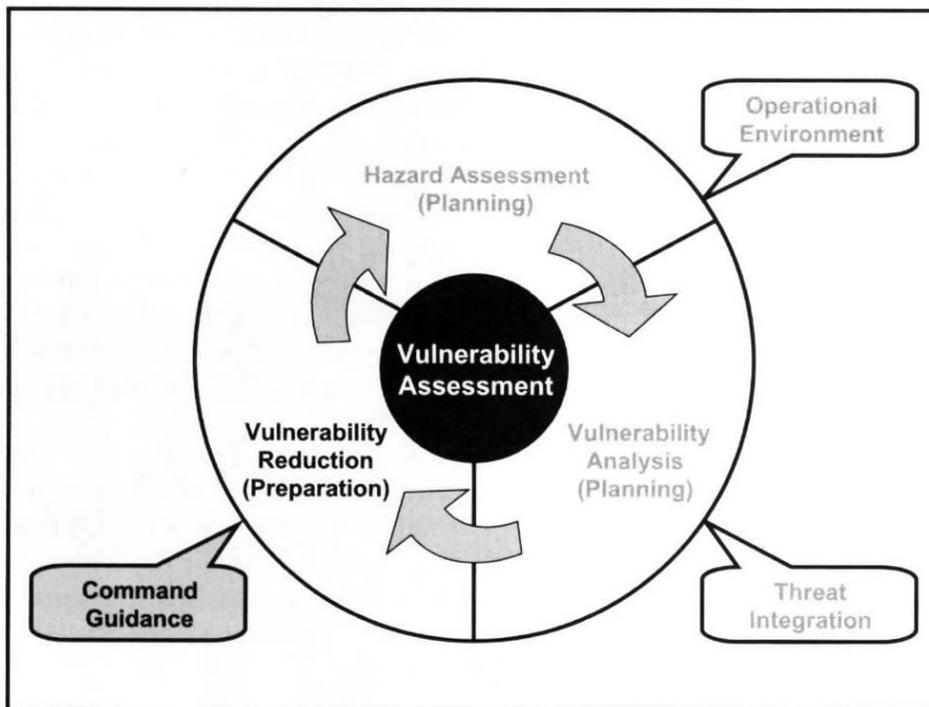


Figure III-2. Vulnerability Assessment During the Preparation Phase

8. Threat Advisory Systems

a. Installation preparedness includes tracking and disseminating information about the threat environment. The installation uses different means to track and disseminate specific threat and CBRN information. These mechanisms are considered for incorporation into the installation CBRN defense plan.

b. DOD Force Protection Conditions (FPCONs) (see Table III-1). FPCONs are graduated categories of measures or actions that ICs can use to protect personnel and assets from attack. Based on factors such as anticipated changes in the threat, changes in the installation VA status, or guidance from higher HQ, an installation may

raise or lower FPCON levels; however, subordinate commanders may raise but not lower a higher-level commander's FPCON. The installation may have access to other information sources that can provide input to what FPCON should be established. For example, ICs may use the following:

- (1) The DOD Terrorist Threat Level Classification System to identify the terrorist threat in a specified overseas area. Installation planners may use this general threat level as one basis for developing FP plans; however, threat levels are estimates, with no direct relationship to specific FPCON.
- (2) The NATO CBRN threat level.
- (3) Other local FPCON systems (e.g., HN force protection alert systems).
- (4) CBRN threat levels. CBRN threat levels serve as a marker for establishing the level of CBRN threat posed by an adversary. CBRN threat levels should be in accordance with Standardization Agreement (STANAG) 2984. FM 3-11.14 provides CBRN threat levels and protection according to STANAG 2984. Table III-2, provides an overview of the CBRN threat levels.

Table III-1. FPCONs

FPCON	Description
Normal	Local security measures designed for implementation when there is no credible threat of terrorist activity. Under these conditions, only a routine security posture designed to defeat the routine criminal threat is warranted.
Alpha	Applies when there is a general threat activity against personnel and/or installations, the nature and extent of which is unpredictable, and circumstances do not justify full implementation of FPCON BRAVO.
Bravo	Applies when an increased or more predictable threat exists.
Charlie	Applies when an incident occurs or intelligence indicates some form of threat against personnel and/or facilities is likely. Implementation of FPCON CHARLIE measures for longer than a short period will probably create hardships for personnel and affect the peacetime activities of units and personnel.
Delta	Implementation applies in immediate area where a threat attack has occurred or when intelligence indicates terrorist action in a specific location is imminent. Implementation of FPCON DELTA normally occurs for only limited periods of time over specified, localized areas.

Table III-2. CBRN Threat Levels

CBRN Threat Level	Description
Zero	The belligerents have no known offensive CBRN capability.
Low	The belligerents have an offensive CBRN capability, but there is no indication of its use in the immediate future.
Medium	Nuclear, biological, or chemical weapons have been used in another AO or there are strong indications that the belligerents will use these weapons in the immediate future.
High	Nuclear, biological, or chemical attack is imminent.

Chapter IV

INSTALLATION CBRN RESPONSE

1. Fundamentals of Installation Response

Each installation response occurs under different circumstances and with different actions. An installation response depends on whether the installation is in a peacetime or contingency environment, what organic resources are available, what resources must be obtained from off the installation, and the threats currently facing the installation. Response forces act in different ways and along their own specific time sequences. See Figure IV-1 for the Response Phase relative to the other phases of Installation CBRN defense.

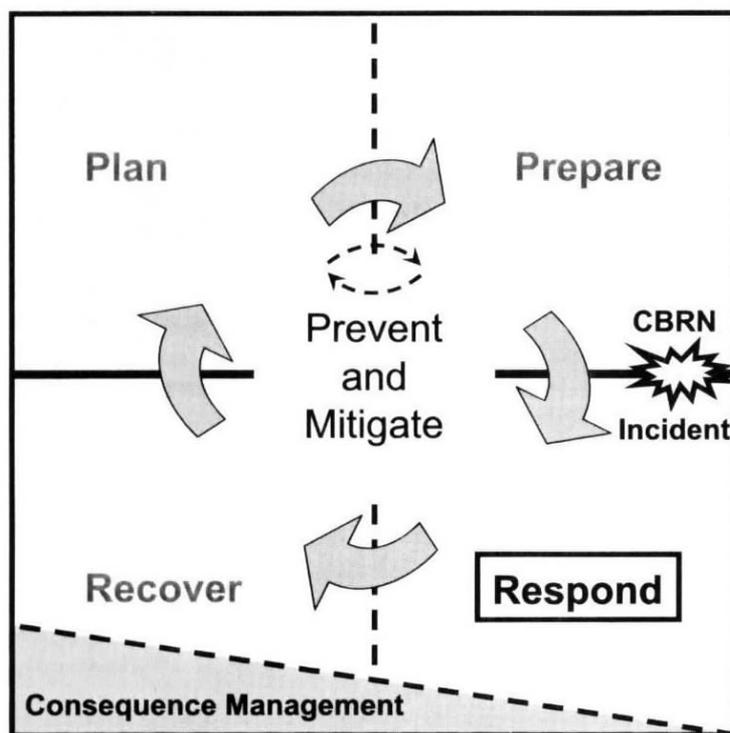


Figure IV-1. Response Phase for Installation CBRN Defense

a. Response Time Spectrum Overview.

(1) The sequence and time of response events varies depending on whether the installation is in a peacetime or contingency environment, the C2 response organization established, based upon the environment, magnitude of the CBRN event and the resources immediately available. Table IV-1 provides a general flow of events for an installation CBRN response.

Table IV-1. Flow of Events for Installation CBRN Response

Trigger	A CBRN incident occurs that requires an installation CBRN response.
First Response	Installation first responders or reconnaissance teams activate.
Initiate ICS	First responders or reconnaissance teams identify the need to establish ICS.
Command Established	Senior official or commander takes charge of the incident.
Notify	Senior official or commander notifies installation leadership. Installation notification procedures are executed. Installation notifies higher HQ as appropriate.
Secure Site/Control Access	Installation first responders or reconnaissance teams identify perimeter and senior official or commander directs perimeter enforcement.
Establish Incident Command Post	Senior official or commander determines need for and establishes, if required, an on-scene ICP; location is disseminated to higher headquarters and local officials. Incident reporting begins.
Task Organize	Available response resources are organized under senior official or commander.
Deploy Response Assets	Responders begin operations based on capability and size of the incident. Requirements for additional response assets requested to higher HQ as appropriate (through EOC).
Follow-On Response Asset Coordinated	EOC coordinates with ESF leads for additional response assets. MOAs/MOUs are executed.
Follow-On Response Assets Arrive	Follow-on response assets report to ICP and are deployed as appropriate. Senior official or commander may change hands as other response assets arrive.

(2) An example of a flow of response events on an installation during peacetime is depicted in Figure IV-2. The figure depicts an installation that must rely on its own resources and those of the theater and HN to completely respond to a CBRN incident—in this case exposure to an unknown white powdery substance in a mail room.

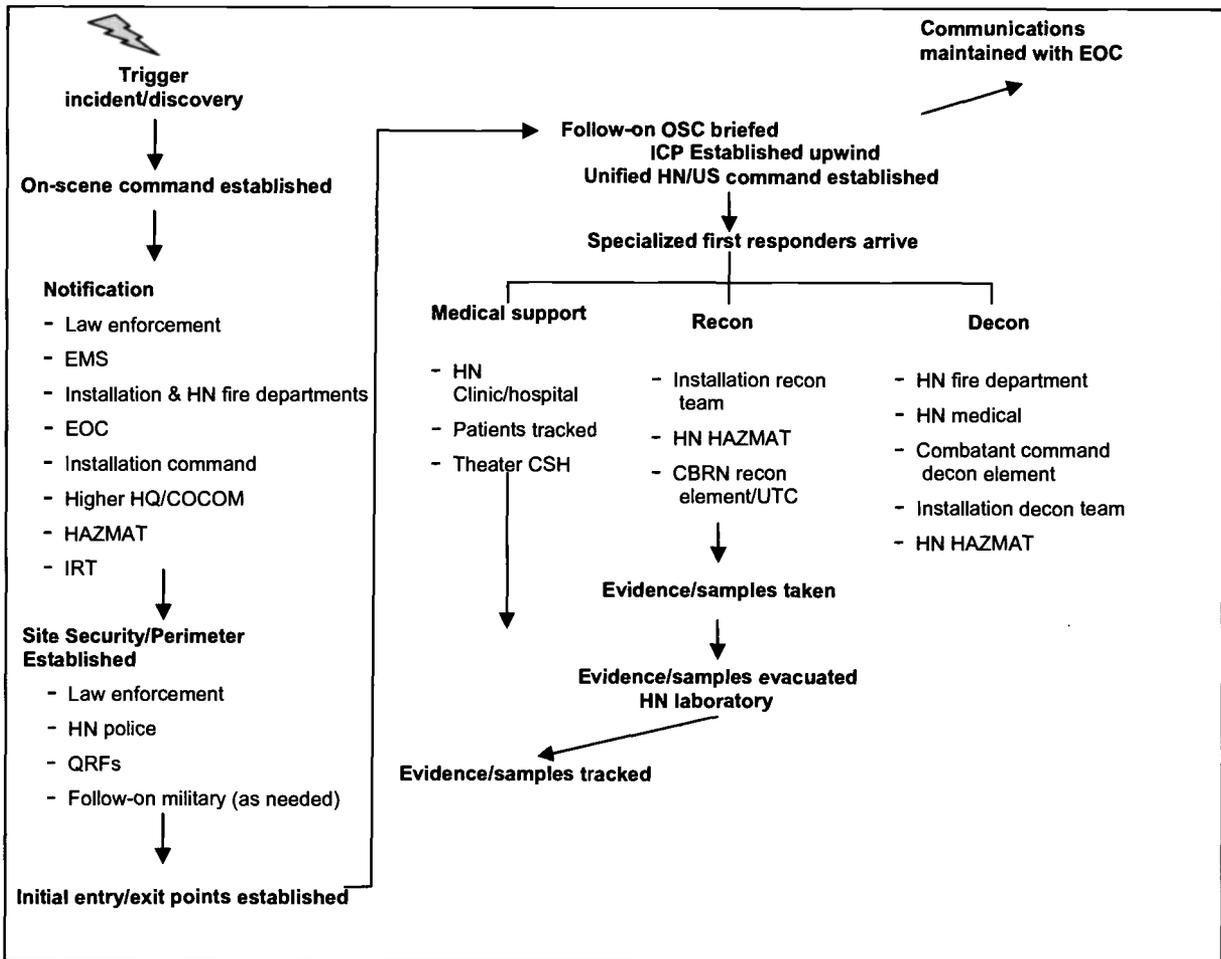


Figure IV-2. Installation Response Example

b. **Triggering.** In simple terms, triggering refers to the initial event or sequence of events, which causes response actions to begin. From an operational standpoint, the installation CBRN vulnerability assessment evaluates the threat and determines when, where, and how each specific threat may employ CBRN agents against the installation or the local community. In response to a CBRN threat with unknown factors, the applicable OPLAN and/or OPORD outlines the priorities of effort and trigger events (decision points) that will result in a CBRN response. Trigger events help determine when response to the incident begins. A trigger may prompt either immediate or delayed response action by responders or the general installation populace. Notification, warning and reporting will implement protective actions to prevent exposure of resources. Knowing when a trigger occurs helps shape the ability of the force to respond. Effective response will drive a more effective recovery phase, limit the severity of the CBRN event on operations, and reduce the overall number of casualties.

(1) **Detector trigger events** refer to the discovery by a detection device signal that a CBRN agent may be present in the environment. CBRN agent detection is limited due to the inherent design of the detector's capability to detect a variety of CBRN agents across the spectrum from specific to generic, as well as the concentration or dosage of CBRN agent detectable threshold (e.g. chemical mass spectrometer with gas-chromatography

vs. chemical detection tape). They may not indicate the presence of all CBRN agents, due to the sensitivity of the devices and the possibility of false positive and false negative readings.

(2) Weapons event triggers refer to an overt attack by a weapons system, such as theater ballistic missiles (TBMs), submunitions, or artillery that might be armed with a CBRN agent. If intelligence has indicated a CBRN-weapons capability, a weapons event in a high-threat area will likely be initially treated as an unknown agent. Detection of an attack in progress may result from an attack warning, a detector alarm, or observable weapons events. The top priority during and immediately after attack should be to determine whether it was a CBRN attack. Detection, observation, or other notices of attack prior to the occurrence of casualties trigger during-attack actions, which are initially focused on immediate resources to preserve human life.

(3) MEDSURV may be the first means of detection for a CBRN event. MEDSURV at its lowest level occurs when an individual identifies the symptoms of a CBRN attack upon an individual and sounds the alarm. At its highest level, MEDSURV could occur through the theater medical surveillance network, where epidemiology is focused on theater-wide tracking of medical symptoms.

(4) Intelligence triggers occur when a commander receives intelligence indicating a threat possesses an offensive CBRN capability, that there is unusual threat activity consistent with operational use of a CBRN agent, or that an installation may be attacked with a CBRN agent. Information and intelligence from multiple sources (e.g., the general public, military intelligence, or national intelligence institutions in the HN) can provide advance warning of a CBRN attack. Intelligence warning is the trigger event that allows a commander the best opportunity to prepare for response.

2. Tiered Response

a. Organization.

(1) DOD installations may use the ICS according to federal law to organize and respond to a CBRN event, depending upon the threat location and environment factors stated earlier. Under circumstances when ICS will be used, the senior installation first responder on the scene at a CBRN incident who has the requisite training implements the ICS (see training requirements below). The responder assumes the role of the IC and is responsible for directing and controlling resources by virtue of explicit legal, agency, or delegated authority. As the installation response further progresses, the role of IC may change hands as more qualified first responders arrive on scene or are appointed by the installation commander. At some point, a unified command may be established depending on the magnitude of the event or an incident of national significance.

(2) The IC is responsible for all aspects of the response, including developing incident objectives and managing all incident operations. The IC sets priorities and defines the ICS organization for the particular response. Even if other positions are not assigned, the IC is always designated.

(3) The IC may assign deputies, who must have the same qualifications as the person for whom they work, as they must be ready to take over IC position at any time.

(4) The organization of an ICS is built around five major management functions—command, planning, operations, logistics, and finance (see Figure IV-3). These functions are applied to any incident, whether large or small. The IC retains responsibility for these functions unless they are delegated to another individual. In some incidents or applications, only a few of the organization functional elements may be formally established or delegated to another individual. However, if there is a need to expand the organization, additional positions exist within the ICS framework to meet any need.

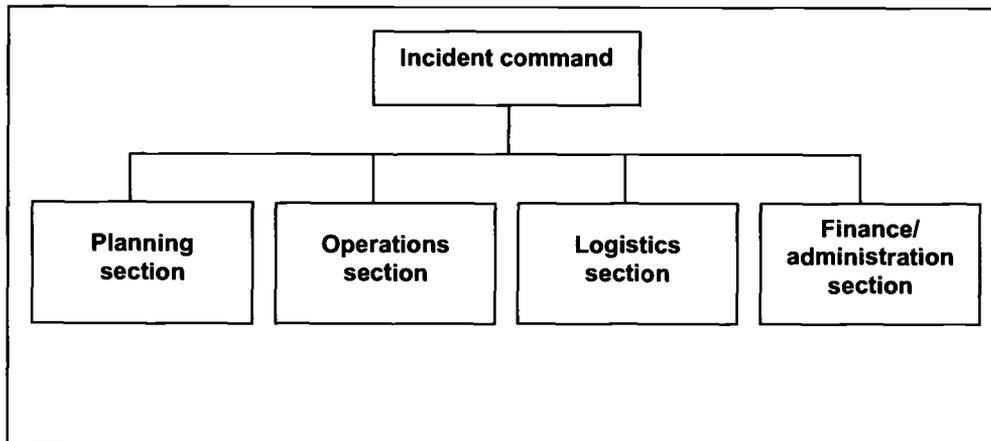


Figure IV-3. ICS Major Management Functions

(5) The modular organization of the ICS allows responders to scale their efforts and apply the parts of the ICS structure that best meet the demands of the incident. In other words, there are no hard and fast rules for when or how to expand the ICS organization. Many incidents never require the activation of planning, logistics, or finance/administration sections, while others require some or all of them to be established. A major advantage of the ICS organization is the ability to fill only those parts of the organization that are required. However, if there is a need to expand the organization, additional positions exist within the ICS framework to meet virtually any need. For example, in operations involving responders from a single jurisdiction, the ICS establishes an organization for comprehensive response management. However, when an incident involves more than one agency or jurisdiction, responders can expand the ICS framework to address a multi-jurisdictional incident.

(6) The roles of the ICS participants also vary depending on the incident and may even vary during the same incident. Staffing considerations are always based on the needs of the incident. The number of personnel and the organizational structure are totally dependent on the size and complexity of the incident. However, large-scale incidents usually require that each component or section be set up separately, with different staff members managing each section. A basic operating guideline is that the IC is responsible for all activities until command authority is transferred to another person.

(7) Another key aspect of an ICS is the development of an incident action plan (IAP). A planning cycle is typically established by the IC and planning section chief, and an IAP is then developed by the planning section for the next operational period (usually 12 or 24 hours in length) and submitted to the IC for approval. Creation of a planning cycle and development of an IAP for a particular

operational period helps to focus the available resources on the highest priorities/incident objectives. The planning cycle, if properly practiced, brings together input and identifies critical shortfalls that need to be addressed to carry out the IC's objectives for that period.

(8) Agencies must be able to use the system on a day-to-day basis for routine situations and for major emergencies.

(9) The senior emergency response official responding to an emergency shall become the OSC/IC of a site-specific ICS. All emergency responders and their communications shall be coordinated and controlled through the OSC/IC, and they shall be assisted by the senior official present for each installation functional area.

(10) The OSC/IC at an emergency response is responsible for controlling operations at the site. As more senior officers arrive (i.e., battalion chief, fire chief, senior law enforcement officials, and IC) the position is passed up the line of authority that has previously been established.

(11) The OSC/IC shall identify, to the extent possible, all CBRN agents, hazardous substances, or conditions present and shall address appropriate site analysis, use of engineering controls, maximum exposure limits, hazardous substance handling procedures, and use of any new technologies.

(12) The OSC/IC shall designate a safety officer who is knowledgeable in the operations being implemented at the emergency response site. He is specifically responsible for identifying and evaluating hazards and providing direction with respect to the safety of operations for the emergency at hand.

(13) Based on hazardous substances and conditions present, the OSC/IC shall implement appropriate emergency operations and ensure that the personal protective equipment (PPE) worn is appropriate for the hazards expected to be encountered.

(14) Responders who are engaged in CBRN defense and emergency response that are exposed to hazardous substances of unknown quantities shall wear a positive-pressure self-contained breathing apparatus (SCBA). They will continue to wear SCBA until the IC or designated safety officer determines a decreased level of respiratory protection will not result in hazardous exposure.

(15) The OSC/IC shall limit the number of emergency response personnel at the emergency site, in those areas of potential or actual exposure to incident or site hazards. Personnel will be limited to those who are actively performing emergency operations. However, operations in hazardous areas shall be performed using the buddy system in groups of two or more.

(16) When the safety officer determines that activities involve an imminently dangerous condition, he shall have the authority to alter, suspend, or terminate those activities. The safety officer shall immediately inform the OSC/IC of any actions needed to correct these hazards at the emergency scene.

(17) After emergency operations have terminated, OSC/IC shall implement appropriate decontamination procedures.

(18) There are two functional centers on the installation during a CBRN incident. They are the incident command post (ICP) and the emergency

operations center (EOC). The ICP is responsible for on-scene response activities, while the EOC is responsible for the entire installation-wide response to the event. During an incident, the EOC provides overall C2 (on behalf of the installation commander) of a CBRN incident. In this role, the EOC functions as an ICS liaison coordinating support for the IC/ICP in all functional areas and follow-on elements (FOE) (see Figure IV-4). The EOC controls all functional-area response and installation support elements so that taskings or requests from the incident site are supported and keeps higher HQ informed.

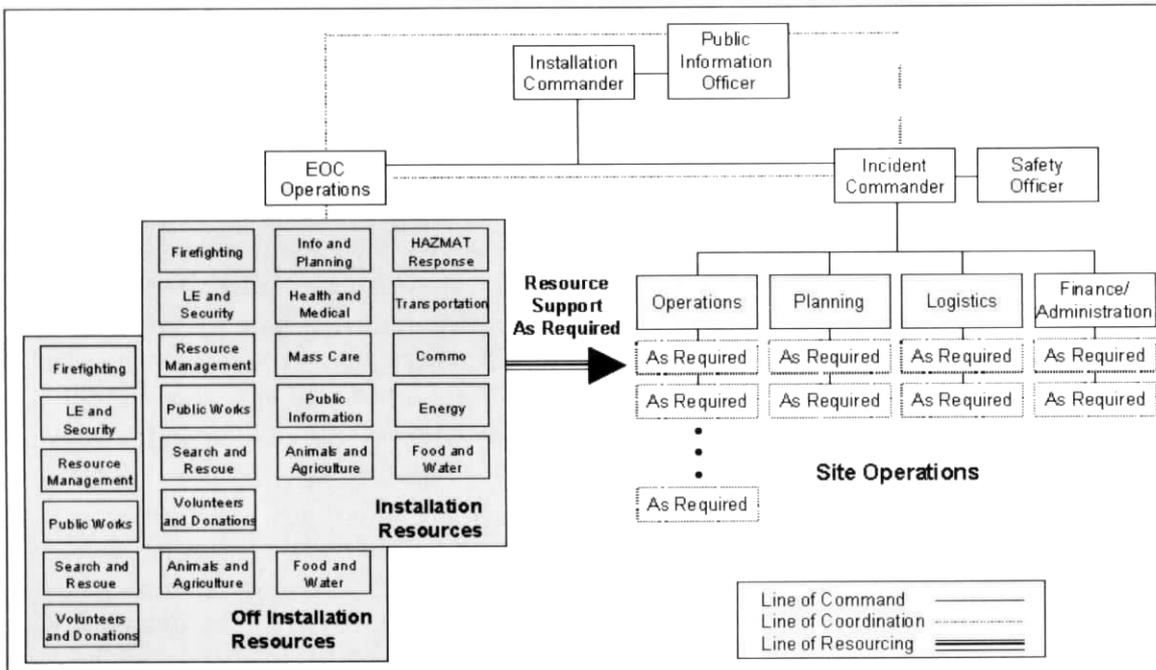


Figure IV-4. Installation Incident Command System

b. **Individual Response/Actions.** Individual response occurs when individuals respond to a CBRN attack by taking appropriate protective actions. The basic response begins with the individual identifying a potential CBRN hazard, donning a protective mask, and sounding an alarm. Individual response may be furthered by donning protective clothing and performing immediate decontamination, self aid, and buddy aid, if required. Further individual response actions are described in Appendix C.

c. **Collective Response/Actions.** Collective actions are coordinated actions in which groups of people respond to achieve a collective goal. An example would be when a unit conducts decontamination of its personnel and equipment after a CBRN attack. Tenant and transient units should be prepared to execute collective actions to mitigate CBRN effects on themselves and to support common installation CBRN responses. Further collective response actions are described in Appendix C.

d. **First Response.** First response is conducted by local and nongovernmental police, fire, and emergency personnel who are responsible for the protection and preservation of life, property, evidence, and the environment. They include emergency

response providers and emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations. First responders may include personnel from federal, state, local, tribal, or nongovernmental organizations (NGOs). In its most basic form, first responders are individuals who are likely to witness or discover a hazardous substance release and who have been trained to initiate an emergency response sequence by notifying the proper authorities of the release. In its more advanced form, first responders are trained to operational or technical levels as presented in Chapter III. Additional first responder actions are described in Appendix C.

e. **Emergency Response.** Emergency response occurs when responders from outside the immediate release area deploy to an occurrence which resulted in, or is likely to result in an uncontrolled release of a hazardous substance. Responses to releases of hazardous substances where there is no potential safety or health hazard are not considered to be emergency responses.

f. **Installation Response.** When a CBRN incident is detected, trained installation personnel initiate the ICS and establish an ICP for on-site response. The ICP is the tactical-level, on-scene incident command and management organization, typically located at or in the immediate vicinity of the incident site. The installation EOC can serve as the operational-level command post where resources are coordinated, command and staff decisions are made, and reporting to higher echelons of command outside of the installation occurs. An alternate EOC site is recommended in the event that the installation EOC is within the hot zone or otherwise inaccessible during an incident.

g. **External Response.** The magnitude of a CBRN attack may quickly overwhelm the ability of an installation to effectively respond. When this occurs, the installation must be prepared to reach out to obtain external support. The external response assets that an installation has coordinated for through MOAs/MOUs should be listed in the CBRN defense plan. This includes assets available through higher commands. Appendix B provides a list of reach-back asset points of contact (POCs) that may provide assistance. Theater-level assets may also be utilized during such an incident. For example, a theater CBRN defense company could be identified in theater concept plans (CONPLANS) to provide assistance. The time it takes to get such external support on-site is critical and must be a primary consideration when planning for such use. Some support will take days to obtain and may no longer be needed once it is available. For example, a unit may be able to provide mass casualty decontamination and processing but may not be able to arrive for a few days. By the time the unit arrives, the casualty processing may well be complete. Time can be a critical factor in handling CBRN patients and their decontamination. External response assets located near the installation are very valuable in that they have the ability to arrive on scene quickly.

3. Emergency Support Functions and Roles

ESFs are used to organize and provide support to the installation CBRN response. This ESF structure can be applied to the installation and its staff. Specific functional personnel should be assigned to lead/manage specific ESF functions. These designated roles are referred to as “ESF managers”. Appendix B provides the ESFs and

some of the ESF manager's roles during a CBRN response. See *Multiservice TTP for CBRN Consequence Management* for additional, more in-depth information. The following are ESF designated for installations:

- No. 1 Transportation
- No. 2 Communications
- No. 3 Public works and engineering
- No. 4 Firefighting
- No. 5 Emergency management
- No. 6 Mass care, housing, and human services
- No. 7 Resource Support
- No. 8 Public health and medical services
- No. 9 Urban search and rescue
- No. 10 Oil and HAZMAT response
- No. 11 Agriculture and natural resources
- No. 12 Energy
- No. 13 Public safety and security
- No. 14 Long-term community recovery and mitigation
- No. 15 External affairs

4. Emergency Communications (Warning and Reporting)

Warning and reporting of an incident occurs at various levels (i.e., individual, collective, and installation levels).

a. Individual. Initial warning that an incident has occurred comes from an individual level to save the lives of those potentially affected or warn those at risk of exposure. The individual may yell, "Gas, Gas, Gas!" and give the appropriate hand and arm signals. Individuals may also report incidents by calling 911 or sending an CBRN1 message.

b. Collective. SOPs at tenant or transient unit level should include how the unit warns of and reports CBRN incidents. The CBRNWRS (see *Multiservice Tactics, Techniques, and Procedures for CBRN Contamination Avoidance*) is normally used by military units to pass CBRN warning and reporting messages. The unit also disseminates a change in its MOPP level to appropriately protect its members. This in itself is a warning (a transient unit commander orders the unit into MOPP4 via internal communications methods).

c. Installation. Installations warn of a CBRN incident through various methods. Methods such as the use of sirens, flags, public address systems, and signs should be described in the installation CBRN defense plan and disseminated to all that occupy the installation (either tenant or transient). The installation may also have a requirement to pass reports of any CBRN incidents to its higher HQ. Tables IV-2 and IV-3 provide additional guidance for standardized alarm signals for the U.S. and overseas.

Table IV-2. Standardized Alarm Signals for the US and its Territories and Possessions

Warning Or Condition	Signal	Meaning	Required Actions
Attack	3- to 5-minute wavering tone on sirens or other devices.	Attack is imminent or in progress or the arrival of nuclear fallout is imminent.	Proceed immediately to designated shelters or take other appropriate actions. Listen for additional instructions.
Warning	3 to 5 minutes of short blasts from horns, whistles, or other devices.		
Peacetime Emergency Warning	3- to 5-minute steady tone on sirens or long steady blasts on horns, whistles, or similar devices.	Peacetime disaster threat exists. Potential or confirmed hazard to public health, safety, or property.	Tune in to local radio, television, or cable stations for emergency information. Listen to public address systems for additional instructions. Be prepared to evacuate or to take immediate shelter or other appropriate protective actions.
All Clear	Declared verbally by local official agencies.	Emergency terminated.	Resume normal operations or initiate recovery, if applicable.

Table IV-3. Standardized Alarm Signals for OCONUS Bases and Stations Subject to CBRN Attacks

Alarm Condition	If You:	This Indicates	General Actions
Green	Hear: Alarm "green" See: Green flag	Attack is not probable.	<ul style="list-style-type: none"> • Don MOPP0 or as directed.^{1, 2} • Perform normal wartime operations. • Resume operations. • Continue recovery operations.
Yellow	Hear: Alarm "yellow" See: Yellow flag	Attack is probable in less than 30 minutes.	<ul style="list-style-type: none"> • Don MOPP2 or as directed.¹ • Protect and cover assets. • Go to protective shelters or seek the best protection with overhead cover.³
Red	Hear: Alarm "red", or a siren (wavering tone) See: Red flag	Attack by air or missile is imminent or in progress.	<ul style="list-style-type: none"> • Seek immediate protection with overhead cover.³ • Don MOPP4 or as directed.¹ • Report observed attacks.
	Hear: Ground attack or a bugle (call-to-arms) See: Red flag	Attack by ground force is imminent or in progress.	<ul style="list-style-type: none"> • Take immediate cover.^{2, 3} • Don MOPP4 or as directed.¹ • Defend self and position. • Report activities.
Black	Hear: Alarm "black" or a siren (steady tone) See: Black flag	Attack is over, and CBRN contamination and/or UXO hazards are suspected or present.	<ul style="list-style-type: none"> • Don MOPP4 or as directed.^{1, 2} • Perform self-aid/buddy care. • Remain under overhead cover or within shelter until directed otherwise.

¹Wear field gear and personal body armor (if issued) when outdoors or when directed.
²This alarm condition may be applied to an entire installation or assigned to one or more defense sectors or zones.
³Commanders may direct continuation of mission-essential tasks or functions at increased risk.

5. Common Operational Picture (COP)

a. During the response phase, a COP is established based upon plans and preparations and is invaluable for providing the installation commander and his staff with a quick, timely, usable, precise, and reliable view of the status of a CBRN incident. During the response phase, the CBRN COP must be capable of supporting all aspects of the response operations (e.g., hazard locations, evacuation or shelter-in-place requirements and locations, unit CBRN capabilities, unit exposure status, and updated CBRN risk assessments) to the extent possible. A key benefit of a good COP system is that it allows the installation to quickly relay to its tenant and transient units this identical, graphic display of relevant information for SA. The same information can be relayed to local U.S. embassy officials, and it is feasible that embassy personnel could then relay specific details on to host nation's representatives as appropriate. Obviously, to be effective, this COP must therefore be constantly updated through the recovery

phase while transitioning to mission sustainment operations. Updates to this COP are made from detection, identification, contamination marking, and warning and reporting information.

b. Examples of information that the installation's operations staff will want to keep updated include:

- Current IPE requirements for all affected areas.
- Split – MOPP operations (if applicable).
- Survey team input on status of all areas of contamination.
- Potential of secondary explosive devices and the likelihood of blast injury and destruction with any CBRN event, especially radiological/nuclear.
- Status of immediate level decontamination.

6. Transition to Recovery and Immediate Mitigation

a. There exists a fine yet unclear line of when response ends and recovery operations begin. Indeed, recovery often begins while response operations are still in progress. There is a need to clearly distinguish between response and recovery, especially for planning purposes. Additionally, there is most often a "handover" of site responsibilities and authorities when transitioning from the response phase to recovery. For example, a responding Fire Chief may hand over control of the scene to crime investigators, incident investigation teams, or senior officials from on or off the installation.

b. Immediate mitigation actions occur during response operations to reduce the harmful effects of the incident and to decrease risks of damage. For example, a hazardous material response team may dike or divert the contamination from a leaking device or container in order to keep the contaminated contents from affecting populated areas. Each situation presents its own unique opportunities to immediately implement mitigation actions.

Chapter V

INSTALLATION CBRN RECOVERY

1. Fundamentals of Recovery

a. This chapter will focus on the initial recovery operations carried out by installation personnel using installation equipment. These actions can be compared to what NIMS refers to as short term “emergency” recovery activities that set the stage for successful long term recovery. Installation personnel and equipment will likely be the only resources immediately available to commence initial recovery operations. CBRN Consequence Management (CM) operations, in comparison, typically require additional personnel, equipment and capabilities beyond those readily available on the installation. See Figure V-1.

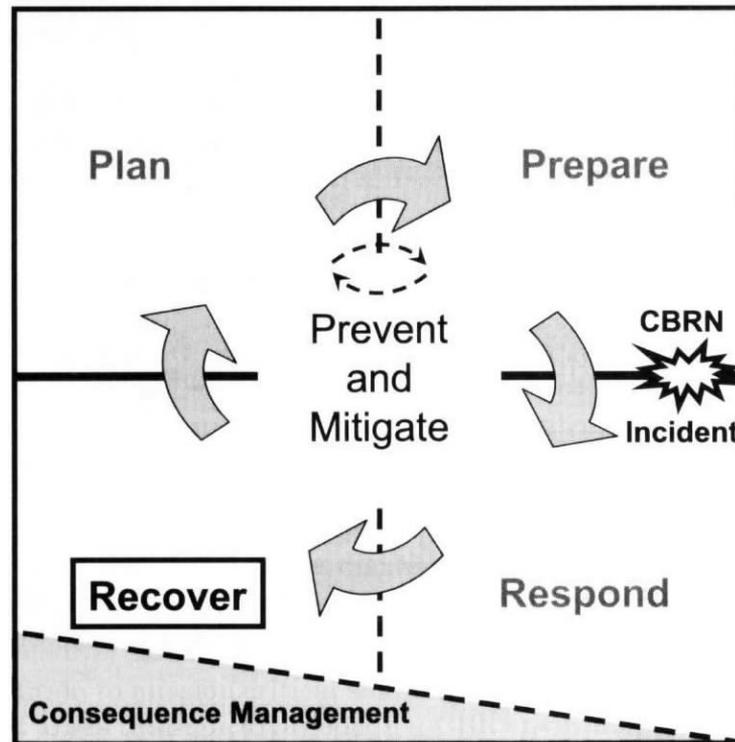


Figure V-1. Recovery Phase for Installation CBRN Defense

b. The DoD Dictionary of Military and Associated Terms (JP 1-02) defines recovery and reconstitution as those actions taken “to minimize the effects of an attack, rehabilitate the national economy, provide for the welfare of the populace, and maximize the combat potential of remaining forces and supporting activities.” The National Response Plan speaks of recovery in terms of “the development, coordination, and execution of service- and site-restoration plans and the reconstitution of

government operations and services through individual, private-sector, nongovernmental, and public assistance programs”.

c. For comparison, JP 1-02 defines consequence management as those “actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents, and JP 3-41 states that “CBRNE consequence management encompasses CM actions taken to address the consequences from all deliberate and inadvertent releases of chemical, biological, radiological, nuclear agents or substances, and high-yield explosives with potential to cause mass casualties and large levels of destruction”.

d. Several key points to remember about the installation’s recovery phase after a CBRN incident are that:

(1) The recovery phase generally begins when immediate hazards are contained or controlled (see Figure I-1).

(2) An installation’s primary tasks during this recovery phase are to complete any remaining mitigation of the immediate hazard, and finish restoring mission capability and essential public and government services interrupted by an event.

(3) By this point after an attack, reconnaissance assets should have determined the boundaries of detectable chemical or radiological contamination, technical reach-back will hopefully have provided assessments of the estimated duration of negligible risk for contamination, immediate and operational decontamination will be complete, thorough and perhaps clearance decontamination will be getting underway, and the installation's ability to carry out its most critical mission-related tasks will have been restored to pre-attack levels.

(4) During this transition to follow-on operations, the installation commander is balancing between focusing resources on mission essential tasks versus completion of recovery tasks. Limitations of resources require the installation’s decision makers to prioritize and concentrate on those tasks needed to recover the installation's missions and operations to full capability.

(5) Many of the recovery tasks initiated by installation personnel during the initial recovery phase will likely be transitioned to CM personnel so that installation personnel can refocus on primary installation missions.

(6) During the recovery phase, installation response teams conduct debriefing operations, begin performing re-supply and equipment maintenance, reset their response posture, and generally reconstitute their operational readiness as they commence / continue their transitions to other tasks.

2. Unique Operational Environment Considerations

As with an installation's CBRN defense planning and its response to a CBRN incident, there will likely be differences in how the recovery operations are carried out depending on whether the installation is in a domestic or foreign setting and whether the installation is in a permissive, uncertain or hostile environment. Listed below are some of the issues that may arise during the recovery phase:

a. **Foreign Installations – Permissive Environment.** Some of the unique factors that the command staff of an installation on foreign territory will need to consider include:

(1) CBRN recovery operations procedures and associated retrograde standards are subject to US and HN agreements that are specified in binding documents such as treaties or SOFAs. These agreements should be fully spelled out, and understood by all responding personnel.

(2) CBRN recovery operations must be routinely coordinated by the installation with their HN civilian counterparts.

(3) Either a permissive or semi-permissive environment may exist during the CBRN recovery operations. Appropriate AT/FP annexes need to be written into each recovery procedure.

(4) Based on the tactical situation at the installation, the commander may assume additional risk and direct the use of MOPP gear, as required. Guidance regarding use of military IPE / MOPP gear must be specifically mandated in writing by the appropriate theater Combatant Commander or higher authority.

(5) Communications linkages to domestically based technical reach-back will likely be more difficult to sustain therefore backup communications paths should be identified.

b. **Foreign Expeditionary Installations – Uncertain or Hostile Environment.** Some of the unique issues that the command staff will likely encounter on foreign expeditionary installations include the following:

(1) CBRN recovery operations could take place in an environment ranging from permissive to hostile.

(2) Based on short-term requirements for support of operational missions against an adversary, crisis-action planning may still dominate recovery operations.

(3) Based on potential shortages of subject matter experts (SMEs) in a hostile setting, the availability of timely technical reach-back may be a critical issue.

(4) At this stage, the possible lack of a robust first-responder capability (e.g., long-term sustainment of recovery operations for days or weeks) may delay or defer recovery operations.

(5) Military IPE is worn during CBRN recovery activities based on written guidance promulgated by the appropriate theater Combatant Commander or higher authority.

c. Domestic Installations. The following are examples of unique factors that any domestic military installation staff will need to consider:

(1) CBRN-related recovery operations occur under the auspices of the civilian-based ICS.

(2) CBRN-related recovery operations occur in a permissive environment.

(3) CBRN-related recovery operations use the same terms of reference used to support first-responder decontamination operations.

(4) CBRN recovery operations are routinely coordinated with civilian counterparts at the federal, state, or local level, as applicable.

(5) CBRN specialists maintain the certification required to operate with civilian first responders (as necessary).

(6) Based on the type of hazard, CBRN responders will be required to wear Level A and/or Level B clothing in lieu of MOPP gear, which don't meet Occupational Safety and Health Administration (OSHA) requirements.

3. Recovery Phase Command and Control

As was stated previously, during the recovery phase, the installation commander must focus his/her resources on those tasks that will most efficiently restore the installation's missions and operations to full capability. Two closely related critical components that help a command's staff efficiently carrying out these responsibilities are an effective information management (IM) program and a well designed and fully functional common operational picture (COP) system.

a. Information Management. An effective installation CBRN IM program provides quality information to the right persons, i.e. installation personnel and tenant and transient units, at the right time in a readily usable form to facilitate understanding and decision-making.

(1) The IM program provides information and direction to impacted personnel, maintains incident management logs and reports, manages data-sharing via interoperability services, supports establishment and operation of any Joint information centers and public affairs offices, maintains all applicable websites or web logs for public use, maintains portals and related data sharing sites for either internal or public use, and performs data-mining activities via available networks. This section is also responsible for appropriate dissemination of intelligence, surveillance, and reconnaissance information, to include threat/hazard warnings.

(2) CBRN IM supports the installation commander in three main areas:

- Achieving SA/understanding.
- Making decisions.
- Communicating execution information to implement those decisions.

(3) This installation CBRN IM has four basic sequential steps that are cyclical in nature:

(a) Identification and update of information requirements. Prior to an event occurring, the command will have developed a listing of critical information that it will need immediately available should a CBRN incident occur. During the response and recovery phases after an incident, those information requirements typically require refinement and updating.

(b) Collection and processing of information. The installation's operations center serves as a central focal point for collecting, processing, storing, protecting, displaying, disseminating key information.

(c) Provide information to build a common operational picture (COP)/display. As events transition to the recovery phase, the requirement to maintain a current COP is even more important. Resource use is probably even more constrained and a single, identical display of information shared by all the commands on an installation is even more important.

(d) Developing an understanding. A common situational understanding (by all parties) is important on an installation to help ensure coordinated and synchronized activities.

b. COP and Intelligence Preparation of the Operational Environment. During the recovery phase, an up-to-date COP is invaluable for providing the installation commander and his staff with a quick, timely, usable, precise, and reliable view of the status of a CBRN incident. During the recovery phase, the CBRN COP must be capable of supporting all aspects of the recovery operations (e.g., hazard locations,

unit CBRN capabilities, unit exposure status, and updated CBRN risk assessments). One key benefit of a good COP system is that it allows the installation to quickly relay to its tenant and transient units this identical, graphic display of relevant information for SA. The same information can be relayed to local U.S. embassy officials, and it is feasible that embassy personnel could then relay specific details on to host nation's representatives as appropriate. Obviously, to be effective, this COP must therefore be constantly updated. Updates to this COP are made from detection, identification, contamination marking, and warning and reporting information. Examples of information that the installation's operations staff will want to keep updated include:

- (1) Current IPE requirements for all affected areas.
- (2) Any ongoing split – MOPP operations (if applicable).
- (3) Survey team input on status of all areas of contamination.
- (4) Information received from technical reach-back (e.g., analysis of CBRN reports).
- (5) Updates on adversary CBRN capabilities.
- (6) Potential of secondary explosive devices and the likelihood of blast injury and destruction with any CBRN event, especially radiological/nuclear. Terrorists may employ conventional explosives in combination with CBR to attract responders to a scene or to injure responders after they respond to a CBRN scene.
- (7) Potential for residual hazards such as breakdown products from CW agents.
- (8) Status of thorough or clearance decontamination.

4. Mitigating CBRN Hazard Effects

As stated above, an installation's primary tasks during the recovery phase of a CBRN incident are to complete any remaining mitigation of the immediate hazard and finish restoring mission capability and essential public and government services interrupted by the event. This must be done while maintaining the safety and protection of affected and responding personnel. Key activities that continue or are initiated during the recovery phase include decontamination, personnel and equipment protection, contamination marking, mortuary affairs, equipment retrograde, and hazardous waste disposal. Although the jobs of completing many of these tasks gradually transitions to CM personnel, installation personnel will likely have initiated each activity. Each of these key activities will be discussed separately below:

- a. Decontamination. Decontamination is conducted as a series of graduated steps (immediate, operational, thorough, and clearance decontamination). The

progression of these steps is dependent on many factors including the operational situation, type of hazard and location of the event. See the *Multiservice Tactics, Techniques, and Procedures for CBRN Decontamination* for much more detailed guidance and TTPs for CBRN decontamination.

(1) Decontamination Status. By the time the recovery phase has begun, immediate decontamination will have taken place to minimize casualties, save lives, and limit the spread of contamination. It is also likely that operational decontamination will have been carried out on specific parts of much of the installation's operationally essential equipment, materiel and/or working areas in order to minimize contact and transfer hazards and to sustain operations. Operational decontamination can also include decontamination of the individual beyond the scope of immediate decontamination, as well as decontamination of mission-essential spares and limited terrain decontamination to reduce penetration of the agent(s) into surfaces.

(2) Thorough Decontamination. During recovery operations, thorough decontamination measures commence in key locations as part of a reconstitution effort; however, these operations require immense logistical support and are manpower-intensive. Thorough decontamination is carried out by a unit, with or without external support, to reduce contamination on personnel, equipment, materiel, and/or working areas equal to natural background or to the lowest possible levels, to permit the partial or total removal of individual protective equipment and to maintain operations with minimum degradation. This may include terrain decontamination beyond the scope of operational decontamination.

(3) Clearance Decontamination. Clearance decontamination is the final level of decontamination. It provides the decontamination of equipment and personnel to a level that allows unrestricted transportation, maintenance, employment and disposal. It is the most resource-intensive and requires command involvement, guidance, and decisions on the disposition of possible mission-essential equipment. Because clearance decontamination involves factors such as suspending normal activities, withdrawing personnel, and obtaining materials and facilities that are not normally present, it will not be discussed here further. Clearance decontamination requires the application of appropriate federal or international standards. The MTTPs for CBRN Aspects of Consequence Management and CBRN Decontamination should be consulted for additional information on clearance decontamination.

(4) Facilities Decontamination. As the recovery phase begins, the installation COP should be indicating what buildings (interior and exterior) were contaminated and what type of contamination is present. The evaluation of sampling results to determine the extent of contamination may also have been completed at this point. Based on evaluation results, it may be possible to resume the use of facilities that were originally isolated and secured during the response phase, or part or all of specific facility functions may need to be transferred elsewhere. Another difficult challenge for the installation is that facilities (exterior and interior) contain many porous surfaces that may absorb contamination and may not be able to be completely decontaminated. Measures such as removal or sealing (painting) of these surfaces are

not options that would likely be exercised by the installation. Rather, these clearance decontamination issues should be left to external CM specialists.

(5) **Terrain Decontamination.** Hopefully as the recovery phase of a CBRN incident commences, reconnaissance assets will have determined the boundaries of detectable chemical or radiological contamination on surrounding terrain. The commander has multiple options available to cope with contaminated terrain including isolating the area, setting revised boundaries for sectors or zones, and decontaminating the terrain. For further discussion on this issue, see the MTTPs for CBRN Aspects of Consequence Management and CBRN Decontamination.

b. **Individual and Collective Protection.** As the recovery phase begins, multiple active and passive measures should be in full operation providing protection to the installation from CBRN hazards. Within the following paragraphs, several of these protection measures for personnel and equipment will be discussed.

(1) **Personal Protection.** During all phases of an installation's response to any incident, the commander and his staff need to monitor the effects of extended wear of IPE on personnel. They need to continually reevaluate what level of heat stress or psychological burden is likely to result from the continued use of protective clothing and equipment under current environmental conditions. Heat stress is a pathological condition in which the body's cooling mechanisms are unable to dissipate the heat load generated. It is disabling and in early, mild stages causes mental confusion and loss of coordination and concentration. Heat stress rapidly progresses through heat exhaustion to heat stroke, which is a very serious medical emergency. These types of evaluations require the assistance of the command's senior medical advisor and his staff. See *MTTP for CBRN Protection* for additional guidance.

(2) **Personnel Evacuation.** Evacuation operations may have commenced as a component of an installation's initial response actions. As the recovery operations progress, depending upon the extent of the impact of the CBRN incident and the progress of the subsequent decontamination efforts, conditions may start to stabilize to a point that it may become safe for some personnel to move back to their original locations. Based on the feedback from post-attack CBRN reconnaissance, the installation commander may deem it safe for personnel to return to their original duty stations. These returning personnel will need to be kept updated on safe routes of movement as the decontamination efforts continue to avoid accidental contamination or re-contamination. A well executed and widely disseminated COP will significantly improve an installation's ability to keep evacuation ambulances and aircraft free of accidental contamination along their egress routes as well as keep installation personnel free of accidental re-contamination during their return to station.

c. **General Medical Activities, Quarantine, Isolation, and Restriction of Movement.**

(1) **Medical Activities.** During the execution of recovery operations, installations continue to use their existing medical capabilities (i.e., generally Level I

[battalion aid station, expeditionary force medical team, and installation medical department activity] and Level II [division-level, expeditionary force medical teams, and installation medical department activity]). During this phase, first responder capabilities still undergoing high use will likely include advanced trauma management, disease prevention, combat and operational stress control prevention, casualty collection, and evacuation from supported units to supporting medical treatment facilities (MTFs). An installation commander's forward resuscitative care duplicates first responder care and expands services available by adding dental, laboratory, X-ray, and patient-holding capabilities. Surgical capabilities may also be provided at this capability by surgical augmentation teams.

(2) **Quarantine and Isolation.** If a biological warfare (BW) agent was used in the attack, "quarantine" or "isolation" may be needed during the response and/or recovery phases to prevent contact between healthy populations and those either infected or suspected of being infected with an infectious disease. These types of decisions are made after consultation with the command's senior medical advisor. Quarantine involves the detention of an individual or group suspected of having been exposed to an infectious disease until it is deemed that they have escaped infection (usually once the incubation period has lapsed). Isolation is the separation of an infected individual from a healthy population. (The term is usually used to refer to patients in an MTF.)

(3) **Restriction of Movement (ROM).** This is another tool that installation commanders may choose to use to maintain operational effectiveness in the face of an infectious disease, whether natural or intentional (such as a BW attack). The goal is to control the spread of the disease by restricting contact between healthy groups of personnel and those who have, or are suspected of having, contracted the disease. Personnel covered by ROM do not necessarily need to be removed from operations. Rather, ROM should be implemented in such a way as to allow them to continue their mission. Again, these decisions are made with recommendations furnished by the command's senior medical advisor.

d. **Contamination Marking.** Contamination marking is used to provide a warning to installation personnel of the presence of contamination. If contaminated areas weren't sufficiently well marked during the initial reconnaissance after the CBRN incident, such marking efforts should be a high priority during the recovery phase. See MTPP for CBRN Reconnaissance for additional guidance on these procedures. Contamination marking signs are standardized in color, shape, and size (see Figure V-2). The primary (background) color of the marking sign indicates the general type of contamination. The secondary (foreground) color identifies the specific hazard. Contamination marking signs are annotated with important information that includes the following data fields:

- **Chemical.** Post the name of the agent, if known, and the date and time of detection.
- **Biological.** Post the name of the agent, if known, and the date and time of detection.

- **Radiological.** Post the dose rate, the date and time of the reading, and the date and time of the burst, if known.

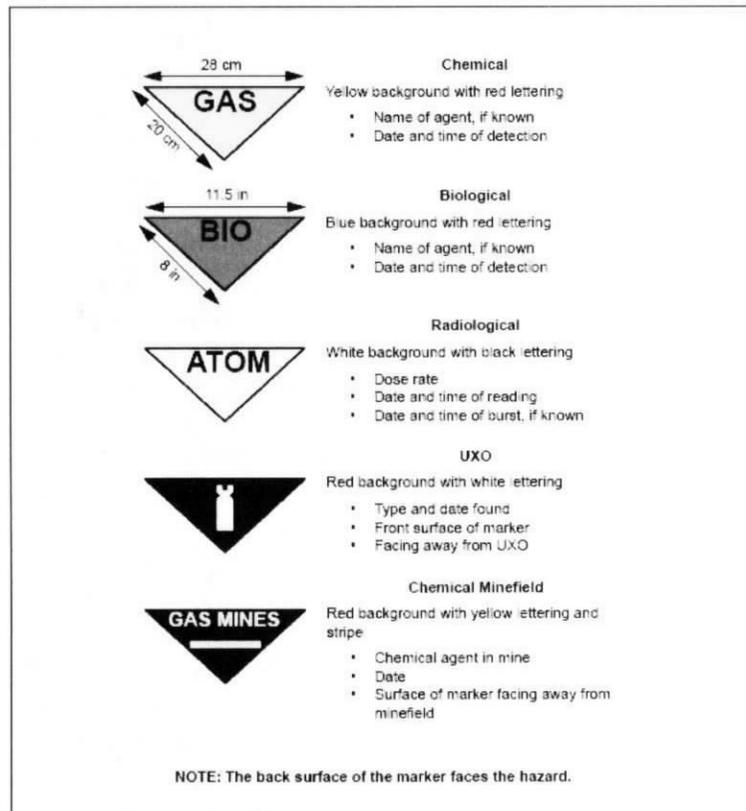


Figure V-2. Contamination Marking Signs

(1) When those standards are not provided or when standard markers are unavailable, units may use expedient markers to mark CBRN hazards. Any suitable material including locally produced marking signs, decals, tape, chalk, and paint may be used to construct these expedient markers to the approximate size and shape of the examples. See *MTTP for CBRN Reconnaissance* for additional guidance on standardized contamination marking sets and figures illustrating expedient CBRN hazard markers.

(2) Standardized CBRN contamination marking procedures include the following:

(a) Place the contamination markers where they will be most likely seen by approaching individuals and units. Individuals who locate the contamination will place markers at the point of detection. To prevent forces from missing posted markers and inadvertently entering contaminated areas, place adjacent marking signs at intervals of 25 to 100 meters, depending on the terrain. If marking contamination in open terrain (i.e., desert, plains, rolling hills), raise the markers to heights that permit approaching forces to view them at distances up to 200 meters. *MTTP for CBRN Reconnaissance* shows a sample contamination bypass marker.

(b) Mark contamination on all sides in rear areas to warn follow-on and support units of the hazard. These clear zones (safe lanes) provide greater freedom of movement by rear area forces through or around contamination.

(c) Mark buildings and other facilities that may be contaminated at critical points, such as entry points.

(d) Mark materiel to protect personnel from accidental contamination. Place contamination markers on any unmarked equipment present in the CBRN attack area. Personnel using equipment after decontamination must take precautions against vapor, particulate, and liquid contamination that may be trapped inside filters, assemblies, and joints. The contamination could pose a hazard while equipment is being used or maintained.

e. Mortuary Affairs. Installations may need to contend with CBRN-contaminated remains. The joint tactics, techniques and procedures (JTTP) for the processing and handling of contaminated remains are found in JP 4-06.

f. Equipment Retrograde. Some equipment that has received low-level contamination may be required during a redeployment (retrograde) within the recovery phase. See the *Multiservice Tactics, Techniques, and Procedures for CBRN Decontamination* and the *Multiservice Tactics, Techniques, and Procedures for Chemical, biological, radiological, and nuclear Aspects of Consequence Management* for further information on equipment retrograde. The installation should maintain copies of any records documenting when and how any of its equipment underwent operational and thorough decontamination operations. The key concern is the potential for residual contamination. During recovery, if equipment is to be retrograded under non-emergency conditions from an installation, some of the basic control measures that an installation should consider adopting include:

(1) Using consolidation points for equipment suspected of residual contamination.

(2) Establishing buffer zones around each consolidation point to provide an additional contamination control measure.

(3) Using specialized detectors and monitors to confirm and monitor for contamination.

(4) Providing installation personnel engaged in monitoring and preparation of equipment retrograde with stringent personal protection and specialized detectors.

g. Hazardous Waste. During initial recovery operations and as well as during subsequent associated longer term consequence management operations, the installation will be challenged with handling and disposing of potentially huge amounts of contaminated waste. These contaminated items may include IPE, field gear, M8/M9

paper, components of M291 and M295 kits, pallet covers, bulk plastic, tarps, other contamination avoidance covers, and decontamination solutions. Guidance on proper collection and disposal of these materials is available in the following documents: Occupational Safety and Health Administration (OSHA) Hazard Communication (HAZCOM) Standard, the OSHA Hazardous Waste and Emergency Response (HAZWOPER) Standard, the Resource Conservation and Recovery Act (RCRA), the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), and the Superfund Amendments and Reauthorization Act (SARA). During recovery operations, the installation's hazardous waste handling responsibilities include ensuring that—

(1) Waste collection sites are established, properly marked, reported, and maintained.

(2) Installation personnel apply contamination avoidance techniques and procedures to establish and maintain waste collection points and segregate wastes for localized collection.

(3) The CBRN control center provides technical guidance and oversight for establishing installation contaminated waste disposal areas and marks and plots accumulation points and disposal areas on local area and grid maps.

(4) Medical authorities provide technical oversight and guidance for personal safety and health-related issues.

h. General Logistics Concerns. As the recovery phase progresses, more and more of the installation's operations begin to return to pre-incident levels as the installation restores additional mission capability. Logistics issues that will likely arise during this period include:

(1) Replacing personnel who may have become injured or ill during decontamination operations.

(2) Reordering supplies (e.g., detector paper, decontamination solutions, decontamination kits, and apparatuses).

(3) Maintaining or repairing vehicles and equipment, including recalibrating or replacing detectors and alarms.

(4) Marking used decontamination sites, selecting new decontamination sites, reporting old and new decontamination sites, and recording and reporting previously contaminated personnel and equipment.

(5) Documenting resource expenditures.

(6) Conducting FHP.

(7) Preparing after-action reviews (AARs) and documenting the use of resources.

Appendix A

INSTALLATION CBRN DEFENSE PLAN DEVELOPMENT

1. Background.

The CBRN defense plan is an important document for support of installation preparation, response, and recovery operations.

2. Installation CBRN Defense Plan Development Process

a. Considerations. Important points to consider for developing a CBRN defense plan include the following:

- The development of a comprehensive, integrated, and executable installation CBRN defense plan is the responsibility of the commander.
- Commander involvement is essential.
- The recommended lead for installation CBRN defense plan development is the installation operations officer and his staff.
- No single individual should be tasked with the sole responsibility of developing an installation CBRN defense plan. Installation CBRN defense plan development and documentation should be a collective effort.
- The most effective method of developing and documenting an installation CBRN defense plan is through the utilization of a cross-functional working group, such as the installation AT working group. This working group should include those individuals (or office representatives) of the ESF managers identified by the commander.
- Using the AT working group ensures the participation, input, and “buy-in” of necessary cross-functional SMEs.
- Everyone involved in installation CBRN defense plan development and documentation should be thoroughly familiar with—
 - Applicable installation CBRN defense directives.
 - Previous installation CBRN defense plans and assessments.
 - Data developed earlier in the overall installation defense plan development process.
- The unpredictability of the installation CBRN defense mission requires that the installation CBRN defense plan provide the “what” and the “how to” instructions that define when, where, by whom, and in what manner specific CBRN defense measures must be conducted and coordinated. Detailed “how to” instructions should—
 - Permit subordinate commanders to prepare supporting plans.
 - Focus on subordinate activities.
 - Provide tasks, activities, constraints, and coordinating instructions.
 - Not inhibit initiative.

- Provide a clear, concise mission statement.
- Convey the commander's intent.
- Include annexes/appendixes, if required, in order to expand the information not readily incorporated in earlier text.

b. Process. The CBRN defense plan format follows the standard OPLAN and five-paragraph order format, yet is tailored to meet the unique requirements of comprehensive CBRN defense programs. There are eight basic steps in developing an installation CBRN defense plan. They are:

(1) Gather/compile information developed during earlier installation planning processes. Information gathered by the planning staff during the entire installation AT/FP planning process is used for CBRN defense plan documentation.

(2) Produce a summary and basic plan. The plan summary provides the reader with a concise synopsis of the scope and purpose of the plan. The basic plan provides the groundwork for all amplifying sections (annexes/appendixes) and is produced prior to their documentation. The basic plan follows the five-paragraph-order format and describes the situation–mission–plan for execution (commander's intent, CONOPS, tasks, coordinating instructions)–administrative and logistics concepts–C2 concepts.

(3) Determine/assign responsibility for developing annexes/appendixes. Annexes provide the details not readily incorporated into the basic plan, and they are written to increase the clarity and usefulness of the basic plan: task organization–logistics–intelligence–personnel–operations–multitude of installation CBRN defense specific topics. These are only required if deemed necessary. Each annex relates to a specific aspect of the CBRN defense operation. Appendixes further expand the annexes and contain even more detailed explanation of the commander's concept for installation CBRN defense operations. Appendixes can further be subdivided into tabs and enclosures. Development and documentation of individual annexes/appendixes should be tasked to the AT working group members with a related expertise or responsibility for the activity. For example, the public affairs representative should supervise the development of Annex F (Public Affairs).

(4) Establish a plan of action and task suspense dates for completion of annexes/appendixes. Installation CBRN defense plan development and documentation requires a comprehensive, integrated approach and a strong, clear vision of installation CBRN defense program requirements. A realistic plan of action, with suspense dates, drives the efficient development and documentation of the installation CBRN defense plan.

(5) Coordinate staff development and review of the plan. Each service has published guidance concerning deliberate planning, organization, and coordination of staff (FM 5-0, NWP 11, Air Force Manual [AFMAN] 10-401, and Marine Corps Warfighting Publication [MCWP] 5-1).

(6) Finalize the plan and submit it to the commander for review and approval. The finalized plan should be—

- Consistent with the organization/installation mission and responsibilities.

- Oriented on tactical perspective.
- Adequately detailed to provide specific actions to be taken.
- Easily understood.
- Executed quickly and decisively, if required.

After the commander's approval and upon execution, the installation CBRN defense plan becomes an OPORD.

(7) Publish, plan, and task the development of supporting plans. Once the installation CBRN defense plan is published, the next planning cycle begins. The installation CBRN defense plan cannot remain static; rather, as the situation changes, the plan must also change. The installation CBRN defense plan must remain under constant review that it is truly a "living document". Each subordinate and supporting commander who is assigned a task in the installation CBRN defense plan may prepare a supporting plan. Supporting plans are consistent with supporting commander missions and responsibilities. Supporting plans are submitted to the supported commander for review and approval.

3. Installation CBRN Defense Plan Format

Figure A-1, page A-4, provides an example of an installation CBRN defense plan format. As stated above, installations have the flexibility to choose their own formats.

1. Situation.

a. Enemy Situation. Describe threat CBRN weapons and agent capabilities, threat delivery capabilities, and circumstances or conditions supporting threat use of CBR weapons.

b. Friendly Situation. Include tenant and transient CBRN defense capabilities/locations with projected arrival and departure times for transients. Identify CBRN defense task organization and current force protection conditions.

c. Attachments and Detachments. List any HN, local, state or federal emergency support units or assets that have been agreed upon under MOAs.

2. Mission. Describe the mission of CBRN defense. Ensure it is consistent with the commander's intent.

3. Task.

a. Commander's Intent. Describe the intent of the CBRN defense program and mitigation measures to prevent potential threat attack so that loss of life is kept to an absolute minimum.

b. CONOPS. Descriptive overview by ESF of how CBRN defense are executed in response to threat CBRN attacks. Articulate who, what, with what, how, where, and when for each ESF during preincident, incident, and postincident phases of a CBRN event.

(1) ESF #1	Transportation
(2) ESF #2	Communications
(3) ESF #3	Public works and engineering
(4) ESF #4	Firefighting
(5) ESF #5	Emergency management
(6) ESF #6	Mass care, HHS
(7) ESF #7	Resource support
(8) ESF #8	Public health and medical services
(9) ESF #9	Urban searches and rescue
(10) ESF #10	Oil and HAZMAT response
(11) ESF #11	Agriculture and natural resources
(12) ESF #12	Energy
(13) ESF #13	Public safety and security
(14) ESF #14	Long-term community recovery and mitigation
(15) ESF #15	External affairs

c. Execution. Describe critical subparagraphs including—

(1) Tasks to Subordinate Tenant Units. Detailed task assignments to each tenant unit with execution guidance, as required.

(2) HN, Local, State, and Federal Agency Tasks. Tasks must be agreed upon by MOA. Specify those assets that are available to support response/restorative efforts, such as fire-fighting equipment, security, and medical assets.

(3) Rehearsals/Exercises. Plan and execute annual rehearsals/exercises to include threat weapons, location of incident(s), participating units, participating civilian agencies, post-exercise evaluations, and other scenario-related characteristics.

Figure A-1. Installation CBRN Defense Plan Format

d. Coordinating Instructions.

- (1) Minimum MOPP levels and flexibility guidance.
- (2) Contamination avoidance guidance.
- (3) Reiteration/establishment CBRN threat-response measures.
- (4) Chemical and biological early warning and detection systems (include integrated chemical alarm systems and biological systems, if available).
- (5) Reconnaissance and survey team actions.
- (6) Personnel safety criteria.
- (7) Operational exposure guidance.
- (8) Automatic masking/unmasking guidance.
- (9) Reporting requirements.
- (10) CBRN sample collection guidance and transfer points.
- (11) Instructions/procedures for civilian/HN interaction/support.
- (12) Decontamination team actions and priorities.
- (13) Locations of HAZMAT storage and disposal facilities.

4. Service Support.

- a. Contaminated casualty collection points/procedures.
- b. Procedures for contaminated remains.
- c. Location of consolidated CBRN defense equipment.
- d. Locations of field-expedient decontamination supplies/HN support.
- e. Decontamination and MOPP exchange points.
- f. Special contamination control requirements.
- g. Retrograde contamination monitoring sites.
- h. CBRN equipment/supply controlled supply rates and stockage points.
- i. Location of medical CBRN defense items and procedures for issue and administration.

5. Command and Signal.

- a. Warning signals and alarms.
- b. CBRNWRS.

Figure A-1. Installation CBRN Defense Plan Format (continued)

4. Sample CBRN Defense Plan

Figure A-2 provides a sample CBRN defense plan in a different format than the above example.

Copy _____ of _____ copies Utopia, USA 39001-0001 XXXX NOV 2003
<u>APPENDIX 5 TO ANNEX C TO INSTALLATION X-RAY AT PLAN</u>
CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR (CBRN) DEFENSE
Ref: See the Basic Plan
1. <u>Situation</u>
a. <u>General</u> . This tab provides planning guidance for the protection of installation X-ray military members, family members, DOD civilian, and on-base DOD contractors from the effects of terrorist CBRN (including TIM). These devices are commonly known as WMD. Installation X-ray units deployed to other locations follow the CBRN planning guidance for those locations. For the purpose of this AT plan, CBRN defense is focused on deterrence through effective planning, training, and equipping of installation X-ray personnel.
b. <u>Enemy</u> . See Annex B (Intelligence).
c. <u>Friendly</u> . See Annex A (Task Organization) and Annex J (Command Relationships).
d. <u>Attachments/Detachments</u> . See Annex A (Task Organization) and Annex J (Command Relationships). For the purpose of this Annex, attachments/detachments refer to tenant organizations that participate in a response to a terrorist incident that occurs on installation X-ray. Attachments/detachments may also be made up of any HN, local, state, or federal response forces that have been agreed upon under appropriate MOAs, SOFAs, or HN agreements.
e. <u>Assumptions</u> .
(1) See the Basic Plan.
(2) There is an increased possibility of a CBRN attack due to the relative ease of access to chemicals, explosives, and plan designs for such devices.
(3) A CBRN scenario exceeds the crisis response/CM capabilities of base resources.
(4) Extensive DOD, local, state and federal support is required to cope with a CBRN scenario.
(5) Incidents involving CBRN are often a combination of three types of incidents. Potentially, they could be HAZMAT incidents, mass casualty incidents, and criminal incidents.
(6) CBRN incidents pose significant problem for first responders.
(7) Installation X-ray should be able to contain CBRN incidents until the arrival of DOD, state, and federal response forces.

Figure A-2. Sample Installation CBRN Defense Plan

(8) Mass casualty planning should augment CBRN planning.

(9) Effective planning, proactive passive/active protective measures, and continuous exercising of crisis action plans help to mitigate the effects of a CBRN attack.

(10) Installation X-ray maintains MOAs with appropriate local, state, and federal agencies or HN forces.

(11) Procedures and protective equipment are required for first responders (i.e., emergency medical services, firefighters, and military police). These can include MOPP, OSHA Level A equivalent, detection equipment, and a heightened awareness for the presence of CBRN agents/devices.

(12) The FBI has primary jurisdiction for investigating CBRN terrorist incidents, and the FEMA is primarily responsible for CM.

2. Mission

On a continuing basis and in conjunction with local, state and federal agencies, installation X-ray is prepared to respond to a CBRN incident and maintains a high level of readiness by conducting preincident planning, implementing mitigation measures, and exercising terrorist incident response/CM operations aimed at lessening the effects of a CBRN incident.

3. Execution

a. **Commander's Intent.** An example of the commanders intent is as follows: "I intend to develop comprehensive CBRN plans designed to marshal installation, DOD, local, state, federal, and civil resources in an effort to deter, mitigate, and respond to a CBRN incident. The cornerstone of this planning effort will be our ability to conduct proactive deterrent measures prior to a CBRN incident. Plans will specifically address how local, state, federal, and civilian resources will be incorporated into deterrent, mitigation and response efforts. **Endstate:** Installation X-ray has executable plans, personnel are trained to be equipped to execute their responsibilities, and CBRN plans are exercised periodically."

b. **CONOPS.** The installation goal is to protect personnel, materiel, and facilities from a potential terrorist CBRN threat. Installation X-ray protects key assets by deterring potential terrorists from employing a CBRN device as a WMD. The focus is on effective planning, training, and equipping of personnel. Commanders must ensure that their units/organizations have planned for a CBRN event and are adequately trained and equipped. In case deterrence fails, incident response and terrorist CM actions reduces the risk to personnel, materiel, and facilities.

(1) Preincident phase.

(a) All units/organizations appoint, in writing, a CBRN defense officer and an alternate to develop, implement, and supervise the organizational CBRN defense program.

(b) The CBRN defense officer's responsibilities include but are not limited to—

- Coordinating with the intelligence division to ensure that the CBRN threat is identified and that information is disseminated to unit/organization personnel.
- Assessing CBRN readiness and vulnerabilities based upon the threat
- Developing CBRN defense plans and training guidance.
- Coordinating and tracking execution of CBRN defense training.
- Identifying CBRN defense logistical requirements.
- Participating in the installation AT working group.

Figure A-2. Sample Installation CBRN Defense Plan (continued)

(c) All units/organizations develop a CBRN defense plan. The plan should be an annex to the unit/organization antiterrorism plan. Plans should be integrated and supportive of the Installation X-ray plan, the next higher HQ and adjoining unit/organization plans. The plan should address the following areas:

- CBRN vulnerabilities and associated mitigation measures.
- Early warning and detection procedures.
- Survey operations.
- Decontamination operations.
- Individual and collective protection procedures.
- Casualty management and evacuation.
- Issuing of medical CBRN defense items.
- Training requirements.
- Resource requirements.

(d) All units/organizations implement CBRN defense training programs that adequately prepare individuals and units to meet the threat (see Tab B to this Appendix). Units/organizations conduct a CBRN defense exercise at least annually using one or more of the materials or agents characteristic of a CBRN attack. The training should challenge the unit ability to react to a CBRN attack and continue operations.

(e) Units/organizations provide CBRN IPE to critical and mission-essential assigned military personnel and DOD personnel. US contractor civilians are provided IPE as determined by contract or by the commander. Issuance of equipment to civilians, including military dependents, must be consistent with supply availability and with consideration of the individual's exposure risk. Civilian personnel, including dependents, issued IPE must be trained on the proper use of the equipment. They are subject to the same individual training standards.

(f) Installation X-ray specific CBRN FPCON measures are established at all levels of command based on assessment of the CBRN threat. CBRN FPCON actions should consist of graduated levels of CBRN defense measures commensurate with the threat of a CBRN attack.

(2) Incident Phase. First responders perform actions such as containing and controlling the incident site; rescuing survivors; performing hasty decontamination, triage and evacuation; and identifying, if possible, the agent. This phase is complete when the immediate threat has been abated and surviving victims have been evacuated for treatment.

(3) Postincident Phase. This phase involves continuing consequence management actions. The incident site is searched for evidentiary material. First responders and terrorist CM workers may require psychological counseling. Response agencies conduct comprehensive reviews of actions taken in order to improve procedures. This phase is complete when the area is restored to normal operations.

c. Tasks.

(1) Installation X-ray Commander

(a) Ensure that CBRN defense plans are developed, individual and collective training and annual exercises are accomplished. associated resource requirements are identified, and IPE is issued to personnel.

(b) Retain jurisdiction for CBRN incidents until the FBI assumes jurisdiction and be prepared to establish a unified command relationship with responding local, state, and federal agencies.

Figure A-2. Sample Installation CBRN Defense Plan (continued)

(c) Exercise C2 through the CMT.

(d) Employ the CBRN emergency response force and other units to deal with the threat.

(2) Director, Operations Division

(a) Retain primary staff oversight for the development of CBRN defense plans. Ensure that CBRN plans integrate available DOD, local, state, and federal response forces and resources.

(b) Coordinate CBRN defense training and annual exercises.

(c) When directed by the installation X-ray commander, convene the CMT and activate the EOC.

(d) Oversee the development and implementation of FPCON measures.

(e) Initiate the installation-wide mass notification process. Periodically test and exercise the notification process to ensure viability.

(f) Ensure that local, state, and federal agencies are notified when an incident occurs and the EOC is activated.

(g) Coordinate CBRN incident and postincident recovery operations.

(h) Prepare and submit installation AARs.

(3) Director, Intelligence Division (OSI, CID, NCIS)

(a) Ensure that all available sources of intelligence are used to develop a CBRN threat assessment as a part of the overall terrorism threat assessment. At a minimum, consider the following questions:

- Who are the terrorist groups who have used or have the capability to use CBRN?
- Are any of these groups or offshoots of these groups present in the local area?
- What type of agents/materials could be used?
- What are the means of delivery?

(b) Provide daily updates and threat summaries as part of the commander's INTSUM.

(c) Be prepared to support the installation CBRN defense training program, as required.

(4) Director, Medical Services

(a) Ensure that medical personnel are equipped and trained to handle CBRN-contaminated victims. Maintain the capability to execute emergency medical services, to include basic lifesaving measures and procedures to treat CBRN contaminated victims.

(b) Develop and maintain a medical MOA/MOU with local civilian and military medical facilities to provide emergency medical support to CBRN incident response operations.

Figure A-2. Sample Installation CBRN Defense Plan (continued)

(c) Maintain an adequate medical supply for CBRN medical emergencies. Maintain a supply of NAAK (atropine and 2 PAM chloride).

(d) Provide an on-scene medical officer to coordinate/supervise triage and evacuation actions.

(e) Advise local hospitals to prepare for the receipt of CBRN-contaminated victims.

(f) Be prepared to execute the mass casualty plan. Establish a procedure for patient tracking and accountability.

(g) Be prepared to support the installation CBRN defense training program, as required.

(h) Execute the installation-wide vaccination policy.

(i) Monitor local, state, and national disease reporting systems for indicators of a biological attack in an area that could affect the installation.

(5) Director, Public Safety Division (law enforcement and security/fire/emergency response)

(a) Ensure that security, emergency response and fire-fighting personnel are equipped and trained to respond to CBRN contaminated incident scenes.

(b) Ensure that fire-fighting and other emergency response personnel maintain an on-scene capability to identify CBRN agents/materials.

(c) Establish procedures for dispatchers to query/identify incoming calls for potential CBRN incidents.

(d) Provide on-scene C2 per Annex C (Operations) and Annex J (Command Relations). Establish cordon area based on weather conditions.

(e) Be prepared to perform hasty decontamination of victims.

(f) Recommend the activation of the CBRN emergency response force, as required. See ANNEX J (Command Relationships).

(6) Director, Public Works (Facilities) Division

(a) Ensure that CBRN scenarios are incorporated into installation HAZMAT response procedures.

(b) Ensure installation HAZMAT response teams are capable of responding to a CBRN scenario.

(c) Be prepared to dispose of CBRN-contaminated waste material.

(d) Be prepared to test installation drinking water and water drainage areas after a CBRN incident, in coordination with medical/bioenvironmental engineering services.

(e) Provide logistical support per Annex D (Logistics).

Figure A-2. Sample Installation CBRN Defense Plan (continued)

(7) Subordinate and Tenant Unit Commanders and Security Zone Commanders

(a) Establish an effective CBRN defense program in accordance with the requirements outlined in this Tab.

(b) Appoint, in writing, a CBRN defense officer and an alternate officer to develop, implement, and supervise the organizational CBRN defense program. Ensure that the CBRN defense officer accomplishes tasks in accordance with paragraph 3.b.(1)(b) above.

(c) Develop a CBRN defense plan. This plan should be an annex to the unit/organization AT Plan. Plans should be integrated and supportive of the Installation X-ray plan, next higher HQ, and adjoining unit/organization plans. Ensure that the plan includes information outlined in paragraph 3.b.(1)(c) above and see Tab A to this Appendix.

(d) Implement a CBRN defense training program that adequately prepares individuals and units to meet the threat (See Tab B to this Appendix). Unit/organizations conduct a CBRN defense exercise at least annually. The defense exercise should have a threat different from that of the previous year.

(e) Provide CBRN IPE to critical and mission-essential assigned military and other DOD personnel (See Tab C to this Appendix).

d. Coordinating Instructions.

(1) The priority of actions for CBRN incident responders are as follows:

(a) Control/contain incident site and surrounding areas.

(b) Perform rescue operations for survivors.

(c) Decontaminate injured.

(d) Triage and evacuate injured.

(e) Collect and preserve evidence.

(f) Collect and identify the deceased.

(g) Conduct site cleanup and HAZMAT disposal.

(h) Return incident site to normal operations.

(2) The primary responsibility of the installation is the containment of the CBRN agent and the rescue of survivors.

(3) All victims of a CBRN agent attack are hastily decontaminated before evacuation to a medical facility. Patient decontamination is achieved by:

(a) Removal of the victim from the contaminated area (hot zone).

(b) Removal of contaminated clothing.

(c) Rinsing with large quantities of water and/or cleaning with various decontamination solutions.

(4) Identification/classification of chemical, biological, and nuclear materials is obtained by using various detection devices.

(5) The MOA is developed to support this Appendix.

Figure A-2. Sample Installation CBRN Defense Plan (continued)

(6) Deploying units should familiarize themselves with any HN response procedures and/or the base defense plans for any sites where they will be tenants. Once deployed and a CBRN incident occurs, units should seek to tie in with existing unit actions and procedures to assist in recovery, security, and other postincident responses.

4. Administration and Logistics

- a. Administration. See the Basic Plan.
- b. Logistics. See Annex D (Logistics).

5. Command and Signal

- a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).
- b. Signal. See Annex K (Command, Control, Communications and Computer Systems).

I. M. RESPONSIBLE
Commander, Installation X-RAY

Tabs:

Tab A: CBRN Defense Planning Process and Plan Format

Tab B: CBRN Defense Training

Tab C: CBRN Defense Equipment and Availability

Tab D: General Chemical Attack Scenario Analysis (Hazard Prediction and Assessment Capability [HPAC] Analysis)

Tab E: General Biological Attack Scenario Analysis (HPAC Analysis)

Tab F: General Radiological Attack Scenario Analysis (HPAC Analysis)

Tab G: General Nuclear Attack Scenario Analysis (HPAC Analysis)

Tab H: General Toxic Industrial Material Scenario Attack Analysis (HPAC Analysis)

Tab I: General Improvised Explosive Device (IED) Scenario Attack Analysis (HPAC Analysis)

Figure A-2. Sample Installation CBRN Defense Plan (continued)

5. Technical Reach-Back Assets

a. Technical reach-back is the ability to contact technical SMEs when an issue exceeds the installation's capability. Reach-back should be conducted using established installation protocols. Many reach-back resources have other primary missions and are not specifically resourced for reach-back. Issues may include the following:

(1) Nonstandard Agent Identification of CBRN Warfare Agents and TIM. Military responders are trained to detect and identify certain military warfare agents. If a TIM is used, or is suspect, then installation personnel must obtain technical information. This technical information could include persistency, medical effects, or decontamination or protection requirements.

(2) Modeling. During CBRN operations, the spread of contamination must be limited. Technical reach-back can help support detailed analysis of an area to assist in determining downwind hazards locating staging areas, operations centers, decontamination sites, etc.

(3) CBRN-Agent Sample Evacuation. Sample evacuation can be an important part of installation operations. The evacuation of samples can provide the means to obtain critical information for patient treatment. Samples evacuated can also be used as evidence for prosecution.

(4) Hazard Prediction. Technical experts can use modeling to provide a better indication of where vapor, liquid, or aerosolized hazards may occur on an installation.

b. Reach-back can be accomplished through various means, from the telephone to broadband satellites; however, information management protocols and chain-of-command must be followed before using any hot-line number.

Table A-1. Technical Reach-Back Contact Information

NRC, Chemical Terrorism/CB Hot Line	800-424-8802 or 202-267-2675 http://www.nrc.uscg.mil/nrchp.html
DTRA	877-240-1187
AFRRI	301-295-0316/0530
USAMRIID	888-872-7443
USAMRICD	410-436-3277
USACHPPM	800-222-9698 http://www.chppm.com

6. National Response Center and Chemical-Biological Hot Line

a. The NRC mans the hot-line service and serves as an emergency resource for first responders to request technical assistance during an incident. The intended users of the hot line include trained emergency personnel such as emergency operators and first responders (firefighters, police, and emergency medical technicians who arrive at the scene of a CB terrorist incident). Other potential users may include the state EOCs and hospitals that may treat victims of agent exposure.

b. The US Coast Guard (USCG) operates the NRC, and its trained operators staff the hot line seven days a week, 24-hours a day. Operators use extensive databases and reference material and they have immediate access to the Nation's top SMEs in the field of CBRN agents. NRC duty officers take reports of actual or potential domestic terrorism and link emergency calls with applicable SMEs (such as those from the Research, Development, and Engineering Command [RDECOM], or the USAMRICD) for technical assistance and with the FBI to initiate federal response actions. The NRC also provides reports and notifications to other federal agencies as necessary. Specialty areas include the following:

- Detection equipment.
- PPE.
- Decontamination systems and methods.
- Physical properties of CB agents.
- Toxicology information.

- Medical symptoms from exposure to CB agents.
- Treatment for exposure to CB agents.
- Hazard-prediction models.
- Federal response assets.
- Applicable laws and regulations.

c. The CB hot line is a joint effort of the USCG, FBI, FEMA, Environmental Protection Agency (EPA), Department of Health and Human Services, and the DOD. The NRC is the entry point for the CB hot line. The NRC receives basic incident information and links the caller to the DOD and FBI chemical, biological, and terrorism experts. These and other federal agencies can be accessed within a few minutes to provide technical assistance during a potential CB incident. If the situation warrants, a federal response action may be initiated.

d. Local established policies and procedures for requesting federal assistance should be used before contacting the CB hot line. State and local officials can access the hot line in emergency circumstances by calling 1-800-424-8802.

7. Defense Threat Reduction Agency

a. DTRA can provide technical reach-back information and services for on-scene personnel. The focal/coordination point for support is the DTRA EOC (1-877-240-1187).

b. The DTRA Operations Center (OPCEN) enables first responders and service members to deal with CBRN threats through on-line assistance and provides a wideband infrastructure for user support. As part of the Combat Support Directorate of DTRA, the OPCEN is manned 7-days a week, 24-hours a day, and has the requisite communications links to act as the single POC for on-line assistance and the dispatch of other agency resources, as required.

c. DTRA resources can provide support and crisis action planning through modeling and simulation, scenario development, and war game and exercise participation. Representative support that can be provided includes—

- Access to decision support assets for CBRN analysis and consequence prediction.
- Access to high-resolution weather data.
- Access to data files on CBRN materials.
- Access to teleconferencing capabilities and national experts.
- Online collaborative support.

8. Armed Forces Radiobiology Research Institute

The Armed Forces Radiobiology Research Institute (AFRRI) can provide DOD with a technical support capability for nuclear/radiological incidents or accidents. AFRRI can provide multiple services, such as furnishing training to health professionals on the management of nuclear or radiological casualties and/or providing state-of-the-art expertise and advice to commanders following a nuclear or radiological accident involving nuclear weapons, a reactor, or radiological material. AFRRI can also provide

access to biodosimetry and bioassay support to incident responders and local health authorities

9. United States Army Medical Research Institute of Infectious Diseases

The US Army Medical Research Institute of Infectious Diseases (USAMRIID) provides medical and scientific SMEs and technical guidance to commanders and senior leaders on prevention and the treatment of hazardous diseases and the prevention and medical management of biological casualties. The USAMRIID serves as the DOD reference center for identification of biological agents from clinical specimens and other sources. The USAMRIID can provide technical guidance for assessing and evaluating a biological terrorist incident, from initial communication of the threat through incident resolution.

10. United States Army Medical Research Institute of Chemical Defense

The USAMRICD provides medical and scientific SMEs and technical guidance to commanders and senior leaders on the prevention and treatment of chemical casualties. The USAMRICD can provide technical guidance for assessing and evaluating a chemical terrorist incident, from initial communication of the threat through incident resolution.

11. United States Army Center for Health Promotion and Preventive Medicine

The USACHPPM provides a variety of technical, medical, and public health SMEs. SMEs are available to provide direct support to DOD field and installation personnel, as well as commanders and senior leaders regarding the prevention and mitigation of, response to, and recovery from incidents involving CBRN releases. The USACHPPM offers particular expertise relative threat and health risk assessments associated with TIC, TIM, and CWA materials. This includes occupational and public health goals and exposure limits including the delineation of response/recovery action levels (i.e., clean up or clearance goals). CHPPM is also designated as the official DOD FHP archival agency for documentation of exposures to military personnel during deployments.

This page intentionally left blank.

Appendix B

EMERGENCY SUPPORT FUNCTION (ESF) MANAGER ROLES

Sample ESF manager roles are shown in Table B-1

Table B-1. Sample ESF Manager Roles

ESF	Name	ESF Manager Roles
No. 1	Transportation	<ul style="list-style-type: none"> • Advise the IC, ICP, or EOC Director on the availability or limiting factors of transportation resources. • Provide transportation for follow-on team members from the assembly point to the designated Incident Command Post as required. • Coordinate all requests for transportation support. • Coordinate the evacuation of equipment from the incident area. • Request additional transportation resources from local agencies when needed. • Strategically plan for future phases.
No. 2	Communications	<ul style="list-style-type: none"> • Monitor mass notification/public warning system. • Supervise and manage the IC, ICP, and EOC computer networks to ensure they are operational throughout an incident. • Provide communications equipment, as needed. • Coordinate and monitor requests for on-site communications assets. • Coordinate and monitor on-site communications support, as necessary. • Determine on-site operating frequencies. • Monitor communication networks; recommend limiting nonessential use of nets. • Maintain the communications log. • Coordinate communications with other appropriate entities. • Evaluate communications capabilities available to support the incident response. Make a recommendation to the IC/ICP/EOC Director on whether to request additional support. • Liaise with augmentation elements to coordinate communications procedures. • Monitor C4ISR status and advise IC/ICP/EOC Director as it changes. • Strategically plan for future phases.

Table B-1. Sample ESF Manager Roles (continued)

ESF	Name	ESF Manager Roles
No. 3	Public works and engineering	<ul style="list-style-type: none"> • Request and monitor the deployed damage assessment team when requested by the IC. • Ensure water and utilities are available for incident site support • Ensure that environmental expertise/technical assistance is available for the IC. • Ensure additional follow-on support is available if required. • Request follow-on elements from installation or civilian sources • Report public works and engineering activities to the EOC. • Strategically plan for future phases.
No. 4	Firefighting	<ul style="list-style-type: none"> • Request augmentation or mutual aid assistance before fire service capabilities are exhausted. • Per IC request, activate MOAs/MOUs with local/state/federal/HN fire and search and rescue assets for augmentation, not previously activated. • Monitor and obtain expendable equipment status from ICP. Request additional equipment as needed. • Strategically plan for future phases.
No. 5	Emergency Management	<ul style="list-style-type: none"> • Manage the overall operation of the EOC • Provide direct support to the EOC director • Submit incident situation reports to Higher HQs through the Installation Commander • Ensure the control and protection of classified material. • Keep detailed records/logs of decisions and events. • Coordinate support from additional response elements with local civilian Emergency Management Official . • Review and comment on incident lessons learned/after action reports. • Strategically plan for future phases.
No. 6	Mass care, housing, and human services	<ul style="list-style-type: none"> • Arrange for mass care. • Arrange disaster housing for displaced persons. • Arrange for human services. • Strategically plan for future phases.
No. 7	Resource Support	<ul style="list-style-type: none"> • Arrange resource support (e.g., facility space, office equipment and supplies, and contracting services). • Strategically plan for future phases.

Table B-1. Sample ESF Manager Roles (continued)

ESF	Name	ESF Manager Roles
No. 8	Public health and medical services	<ul style="list-style-type: none"> • Ensure emergency medical services are available, as necessary. • Report potential BW incidents to higher HQ. • Request assistance from outside sources, such as the CDC, to confirm diagnosis and to control the further spread of disease. • Ensure medical intelligence officer or NCO is available to provide medical intelligence information if needed. • Advise the IC/EOC/ICP on the status of medical treatment activities. • Coordinate with local medical forces for mutual assistance requirements on scene; activates appropriate procedures if during non-duty hours. • Serve as a liaison with the installation medical facility for on- and off-installation medical needs. • Strategically plan for future phases. • Establish contact with the MCC, Local EOCs and Higher HQ. • Ensure medical personnel are available to provide technical medical information and advice to the IC, including information on physiological effects of contamination. • Coordinate with local hospitals for bed availability. • Establish reach-back guidance and support from USAMRIID, USAMRICD, AFRI, USACHPPM, and CDC. • Establish contact with local, municipal, state, and federal public health agencies, as required. • Establish contact with state/regional/local public health laboratories for LRN support, as needed • Strategically plan for future phases.
No. 9	Urban search and rescue	<ul style="list-style-type: none"> • Activate the Urban Search And Rescue Team • Dispatch team when requested by IC. • Strategically plan for future phases.
No. 10	Oil and HAZMAT response	<ul style="list-style-type: none"> • Activate installation Oil and HAZMAT resources and deploy to incident site when requested by IC • Request from local civilian agencies/higher HQ augmentation if the CBRN/HAZMAT team capabilities are exceeded. • Strategically plan for future phases.
No. 11	Agriculture and natural resources	<ul style="list-style-type: none"> • Advise the IC on natural and cultural resources, and protection/restoration of historic properties. • Strategically plan for future phases.

Table B-1. Sample ESF Manager Roles (continued)

ESF	Name	ESF Manager Roles
No. 12	Energy	<ul style="list-style-type: none"> • Deploy a damage assessment team when requested by the IC. • Ensure backup power is available to the incident site. • Provide functional expertise and assistance to the CBRN/HAZMAT team, as required. • Determine the need for additional follow-on support. • Assist with coordination among the IC, ICP, EOC, and other civil and/or military authorities involved with the response. • Strategically plan for future phases.
No. 13	Public safety and security	<ul style="list-style-type: none"> • Monitor incident site perimeter/cordon security. Deploy additional forces as requested by the IC/ICP. • Coordinate additional civilian Law Enforcement support as needed or requested by the IC/ICP. • Ensure safety of emergency responders and public through monitoring incident situation. Draft and provide safety notices for EOC Director's approval. • Ensure personnel in the immediate area are aware of any potential hazards coming from the site. • Monitor individual equipment items status, especially during CBRNE incidents. Request additional equipment and vehicles to meet the needs of incident site security personnel for sustained operations through the recovery phase. • Request augmentation support from the EOC Director; e.g. Installation commander approval needed to obtain non-emergency responder personnel support to maintain incident site perimeter/cordon security. • Monitor safe routes and advise emergency responders of recommended/needed changes to those routes. • Coordinate installation entry requests with appropriate control centers, agencies, and ESFs. • Strategically plan for future phases.

Table B-1. Sample ESF Manager Roles (continued)

ESF	Name	ESF Manager Roles
No. 14	Long-term community recovery and mitigation	<ul style="list-style-type: none"> • Conduct a social and economic community impact assessment. • Recommend long-term community recovery assistance to states, local governments, and private organizations and individuals that reside on the installation or are affected by an installation related disaster. • Conduct mitigation analysis and program implementation. • Alert and notify a SJA EOC representative to proceed to the incident site or designated assembly point and report to the IC. • Determine whether claims should be activated. • Provide advice and assistance to the installation commander, EOC, IC, and ICP members (as appropriate) on all legal issues arising from incident and the response, including issues associated with establishing an NDA; providing military support to civil authorities; and providing support to civil authorities. • Provide advice and assistance to responding security forces, as appropriate, including advice on chain of custody/evidence preservation issues. • If claims teams are mobilized, prepare estimates of damage and injuries, dollar estimates of third party-damage (if possible), Report the status of funds available at the installation, and determine potential need for advance payment and additional JA manning. • If appropriate, establish a temporary claims office in proximity to the incident site and advertise the location, operating hours, and availability of advance payments. • Strategically plan for future phases.

Table B-1. Sample ESF Manager Roles (continued)

ESF	Name	ESF Manager Roles
No. 15	External affairs	<ul style="list-style-type: none"> • Coordinate with Installation Operations Center (IOC) or Emergency Operations Center (EOC), ICP, and IC for probable timing and location of the establishment of the public information facility. • Activate the press center, as directed by the EOC Director or Installation Commander. Coordinate installation access. • Ensure Public Affairs representation at the Joint Information Center, if established. • Coordinate liaison with media representatives to provide accreditation, mess facilities, billeting, transportation, and escorts, as authorized and appropriate. • Ensure PA liaison and spokesperson is available to the Incident Commander in order to respond to public requests for information. • Coordinate media access regarding the incident. • Coordinate and monitor movement of news media personnel ensuring press passes, escorts, etc. are available. • Coordinate media requests for photographs, interviews, and biographical and other data. • Answer community concerns and deal with the news media at the incident site. Recommend and coordinate an emergency information line/rumor control line. • Prepare, coordinate, and disseminate public information alerts. • Ensure information for public dissemination is reviewed for compliance with security and policy requirements. • Coordinate all public information drafts with the installation commander or the commander's designated representative. • Obtain approval from the installation commander for news releases; the release of photographs of suspects, victims, and the immediate scene; interviews with anyone other than the commander; and direct communication with press personnel and suspects. • Make news release(s) available. • Report the facts concerning the CBRN incident/attack, the government investigation, apprehension of terrorists, recovery operations, and other stories of interest to the public, as appropriate. • Strategically plan for future phases.

Appendix C

INSTALLATION CBRN CHECKLISTS

1. Background.

This appendix addresses two areas. First, installation CBRN checklists and the described actions are provided. The checklists support furnishing an integrated, cross-functional response. Second, this appendix describes representative coordination and information activities that should occur between the installation and tenant and transient units on an installation.

2. Checklists

The CBRN checklists are separated into the following categories:

- Planning and Preparing (see Table C-1). The planning and preparing checklists are combined into one table, as planning and preparatory actions overlap.
- Response (see Table C-2, page C-4).
- Recovery (see Table C-3, page C-6).

Table C-1. Planning and Preparatory Actions

Individuals
Attend Level I AT training course and ensure that accompanying dependents 14 years or older attend course prior to leaving CONUS.
Train to proficiency on all individual CBRN protection tasks.
Leaders (All)
Attend Level II/III AT training course, as appropriate.
Ensure personnel immunizations are up-to-date.
Reinforce individual CBRN survival tasks through continuous training.
Collective (Unit, Team, or Cell)
Participate in CBRN emergency response exercises.
Prepare and maintain personnel, equipment, and supplies fully capable of performing required tasks associated with CBRN/TIM event activities.
Identify CBRN response augmentees in the unit/team/cell by name and have them participate in exercises with the supporting element, as required.

Table C-1. Planning and Preparatory Actions (continued)

Installation Commander
Attend Level III/IV AT training course, as appropriate.
Ensure that responsibilities, resources, and requirements are identified for a successful installation CBRN emergency response plan. Review the CBRN emergency response program and plans at least annually to ensure compliance with standards.
Ensure that the installation CBRN emergency response plan addresses security and/or possible evacuation of DOD personnel and their dependents.
Authorize and direct an evaluation of the CBRN response program to be conducted in order to establish a baseline for the installation. Ensure that the evaluation identifies equipment, personnel, training, exercise requirements, and MAAs needed to coordinate additional response capabilities from local/state/federal/HN organizations
Ensure that a CBRN exercise is conducted annually using realistic CBRN scenarios to validate the CBRN emergency response plan.
Designate an emergency disaster planning officer with CBRN emergency response program management responsibilities.
Align installation exercise and training schedules with local/state/federal/HN CBRN exercises.
Coordinate CBRN emergency efforts on the installation with local/state/federal/HN emergency responders to ensure interoperability.
Direct and ensure that a viable health protection program is established, equipped, and trained.
Direct and ensure that MOAs are coordinated with local/state/federal/HN authorities and that cohesive working relationships are established and maintained through training and sharing of information.
Review MOAs annually to ensure that local/state/federal/HN sufficiency exists in meeting agreed-upon installation emergency response needs.
Review SOFAs and other international agreements affecting CBRN responses and local/state/federal/HN emergency response capabilities.
Installation IOC/EOC Director
Ensure that the installation CBRN emergency response CONOPS includes the establishment of an ICS.
Determine a primary and backup location for the IOC/EOC. Incorporate collective protection systems in facility.
Identify primary and alternate IOC/EOC personnel.
Establish operating procedures for the IOC/EOC, including duties and responsibilities of staff, communication, reports, and timelines for notification to higher HQ.
Establish and maintain current emergency response notification rosters, including rosters of all off-post response agencies. Brief the installation commander on all changes to the rosters.
Establish and ensure the implementation of automated CBRNWRS using preformatted or preaddressed messages for local/state/federal/HN reports. Ensure that personnel are trained on CBRNWRS and networks.
Develop a CBRN emergency response plan that integrates facilities, equipment, training, personnel, and procedures for crisis management and response operations into a comprehensive effort designed to provide the appropriate protection to personnel and critical missions on the installation.
Develop a system for rapid distribution of available CBRN/TIM escape masks to all personnel (military, civilian, dependent) on the installation.

Table C-1. Planning and Preparatory Actions (continued)

Installation IOC/EOC Director
Integrate response functions into the CBRN emergency response plan, including preparedness, public affairs, legal counsel, public works and safety, chaplain services, mortuary affairs, and resource management.
Utilize the most current TIC information from ITF-25 and ITF-40 and site surveys to determine installation priorities for protection from TIM.
Annually identify the full range of known or estimated terrorist capabilities and the possibility of nonhostile incidents for use in conducting VAs and planning countermeasures.
Examine the CBRN emergency response programs and assess written plans and programs designed to support preincident planning, emergency response, medical needs, equipment, law enforcement, training, intelligence support, security, and postincident response.
Examine the availability of resources to support plans as written and the frequency and extent to which CBRN emergency response programs have been exercised. The assessment should determine the status of formal and informal agreements with supporting organizations using an MOU, MOA, inter-service support agreement, host-tenant support agreement, etc.
CBRN VAs should address the IOC, fire and emergency services, medical services, CBRN/HAZMAT team, law enforcement and security personnel, and bomb technicians.
Ensure that CBRN VA includes an inventory of assets on the installation and resources available through mutual-aid assistance with outside communities.
Include participants from all emergency-response functions on the installation and whenever possible, appropriate local/state/federal/HN organizations in exercises.
Incorporate lessons learned from installation emergency response CBRN exercises into the overall installation FP plans.
Identify responsibilities, resources, and requirements needed for successful execution of the installation CBRN emergency response program and integrate these into the plan.
Collect and prioritize installation CBRN emergency response resource requirements for the POM submission.
IOC/EOC CBRN Cell
Coordinate storage, issue, movement, and maintenance of installation CBRN equipment and supplies.
Conduct periodic inventories of CBRN response equipment.
Ensure that installation emergency response equipment is interoperable with equipment used by local/state/federal/HN mutual-aid partners according to DODI 2000.18, whenever possible.
Ensure that a personnel identification and accountability system is established for all response teams to operating at the incident site.
Monitor CBRN/perimeter surveillance devices according to the installation emergency response plan.
Incident Commander/On-Scene Commander
Attend the IC course.

Table C-2. Response Actions

Individuals
Watch for CBRN attack indicators.
Minimize skin exposure.
Proceed immediately to designated shelters and/or assume and maintain MOPP as directed.
Check self/assets for contamination.
Report in for personnel accountability.
Listen for instructions.
Operationally decontaminate self/assets.
Leaders (All)
Disseminate threat and emergency action information, protective measures, and other incident information.
Direct the covering of mission-essential equipment.
Protect facilities by closing all windows and outside air intake, turning off ventilation systems, etc. at the time of attack and implementing single-entry procedures.
Maintain a log of events to document emergency response actions.
Collective (Unit, Team, or Cell)
Initiate personal protection and accountability measures.
Assemble and dispatch unit personnel, as required.
Installation Commander
Initiate increased FPCONs, as necessary.
Monitor all on-scene actions.
Ensure that local/state/federal/HN officials are notified and updated as the situation requires.
Determine if a public health emergency exists on the installation, based on information provided by the PHEO. If it does determine whether the emergency powers listed in paragraphs 4.6. and 4.7., DODD 6200.3, should be implemented.
Decide if and when evacuation of installation facilities is appropriate.
Authorize requests for augmentation, as necessary.
IOC/EOC/CBRN Cell
Activate the IOC/EOC alert procedures and installation alert rosters and recall procedures for the various emergency response teams.
Set up an incident information center for coordination.
Establish and maintain communications with the IC and other responders.
Obtain the initial report from responders and determine the location of the incident.
Track and plot initial incident information on an installation map.
Integrate information from CBRN/HAZMAT team, medical, security, and intelligence assets.
Track and maintain the status of the situation, including record event casualty summary, damage summary, weather status, evacuation status, area closing status, shelter facility status, resources or equipment status, medical facility (base and local) bed availability, and the status of response to contracts or agreements for services.
Activate the installation warning systems. Notify the base populace by emergency alert system or MARS, radio or television, mass notification systems within buildings, the 'Big Voice' outdoor sirens, or other predetermined means in order to direct proper procedures to avoid the incident site (by either evacuating or SIP).
Establish and maintain communication links with higher, lateral, and lower elements.

Table C-2. Response Actions (continued)

IOC/EOC/CBRN Cell
Activate appropriate elements of the MAAs and monitor augmentation from civilian and military forces.
Notify the appropriate EOD control center of the need for EOD support, if required. Coordinate with the transportation representative to provide movement of EOD personnel with special EOD tools and equipment to the incident site by the most rapid transportation mode available, to include military and commercial charter aircraft.
Receive and send orders, information, reports, and requests pertinent to the incident to subordinate commands/agencies, higher HQ, and outside civilian agencies. Serve as the central tasking office for all internal and external taskings regarding the incident.
Issue changes to the FPCON level as directed by the IC.
Maintain an incident log.
Continuously monitor with CBRN/perimeter surveillance devices according to the installation emergency response plan.
Provide COP to the installation commander, IC, other installation offices, and local/state/federal/HN agencies, as required.
Track response assets and effectively manage resources.
Request additional resources to support response through recovery, as necessary.
Incident Commander/On-Scene Commander
Locate and assess the incident site.
Assume command of on-scene operations and perform IC duties until relieved of duties (after security and response forces have neutralized all hostile force terrorist activity).
Establish assembly areas for the incident response team members in a controlled environment and ensure that initial preparation of the incident and team-leading procedures are conducted.
Mark contaminated areas to prevent casualties and the spread of the hazard.
Determine the initial cordon size, based on the type and quantity of material involved at the incident.
Identify safe routes for follow-on forces
Assemble and account for all incident response team members and augmentees.
Establish and ensure that all responders operating in the contaminated areas have the appropriate protective clothing and equipment available and are trained and medically cleared to respond.
Notify all nonessential personnel to evacuate from the incident site.
Ensure that personnel working at the incident site understand all safety procedures for work-rest regimes and protective measures against climatic conditions. Ensure that personnel have adequate food and water and are aware of the location and use of sanitary facilities.
Ensure that comprehensive control, decontamination, and medical intervention activities are in place prior to any response team entry into the contaminated area.
Advise team members to look out for secondary devices such as IEDs/booby traps.
Determine if the incident is a crime scene and initiate procedures to preserve evidence, if required.
Establish initial hot, warm, and cold zones.
Conduct contaminated casualty extraction, in coordination with installation fire and emergency services. Provide triage and emergency medical service, if required.
Search for secondary devices in coordination with EOD.
Detect CBRN hazards.
Identify the CB agent.

Table C-2. Response Actions (continued)

Incident Commander/On-Scene Commander
Collect aerosol, environmental, plant/animal, and medical samples.
Prepare and forward samples to the laboratory for further analysis and identification.
Establish exposure limits and stay times in the area for wearing protective equipment based on agent type, concentration (if known), and ambient temperature. Rotate personnel based on exposure levels and stay times.
Conduct a survey to analyze agent transfer and spread.
Submit incident SITREPs to IOC/EOC.
Maintain continuous communication with the IOC/EOC and provide updates as the situation changes.
Transfer control of the site to the lead agency, as directed. Provide a detailed SITREP to include the product released, operations taken or in progress, call signs, all resources on site, additional resources on call or enroute, and any other considerations.
Ensure the control and protection of classified material.
Keep detailed records of decisions and events.
Accurately record HAZMAT exposure for personnel. Keeping accurate records enables the tracking of long-term health effects on those exposed to HAZMAT.
Coordinate support from additional response elements through higher HQ.
Coordinate with augmentee personnel, follow-on elements, and others who will provide support at the incident site.
Coordinate with the relieving IC when he arrives at the incident scene. Brief the new IC on the situation, including the organization under IC control.

Table C-3. Recovery Actions

Individuals
Avoid potentially contaminated surfaces and areas.
Obtain and report observations and evidence of an attack.
Provide input, as required, to incident AARs.
Return IPE to a ready status in anticipation of another attack.
Leaders (All)
Ensure that unmasking procedures are carried out according to the SOP.
Monitor personnel for unusual physical conditions or symptoms.
Document exposures.
Collective (Unit, Team, or Cell)
Ensure that personnel, equipment, and supplies are prepared to perform required tasks associated with another CBRN/TIM event.
Develop and provide input to incident lessons learned/AARs.
Installation Commander
Oversee recovery operations on the installation.
Review and approve necessary reports following the incident, including lessons learned and AARs.

Table C-3. Recovery Actions (continued)

Installation IOC/EOC/CBRN Cell
Coordinate activities of follow-on elements.
Monitor recovery operations and support the needs of the installation commander.
Coordinate input to the incident lessons learned/AAR.
Write the installation AAR based on input from various functional areas.
Incident Commander/On Scene Commander
Assess the incident site for any remaining hazards and determine the mitigation actions needed. Advise the IOC/EOC and installation commander.
Provide HAZMAT support to the IOC/IC through recovery.
Develop and provide input to incident AARs.
Individuals
Report unusual physical conditions or symptoms.
Leaders (All)
Monitor personnel for unusual physical conditions or symptoms.
Document exposures.
Collective (Unit, Team, or Cell)
Reconstitute unit/team/cell personnel, equipment, and supplies until fully capable to perform the required tasks associated with CBRN/TIM event activities.
Installation Commander
Oversee recovery and reconstitution operations on the installation.
IOC/EOC CBRN Cell
Ensure that installation emergency response equipment is decontaminated or replaced.
Ensure that CBRN filters are replaced after exposure.

3. Installation Tenant and Transient Unit Coordination

Maintaining effective coordination and liaison between the installation, tenant, and transient units is the responsibility of all those concerned. This appendix addresses a representative list of information and coordination measures that a tenant or transient unit should share with an installation on a mutual basis.

a. **Common Considerations.** Adequate preparation and coordination is key to the success of the liaison and coordination activity between the installation and a tenant or transient unit. Coordination must be an integral part of the planning process, and the tenant and transient units must fully understand the installation commander's emergency response plan. Common understandings between the installation commander and tenant and transient units include the following:

(1) Understanding each mission, the coordination and liaison functions, the commander's expectations, and the specific responsibilities between various organizations on the installation.

(2) Becoming familiar with potential issues of the installation (e.g., shortage of first responder resources), including specific issues and CBRN information requirements for the installation staff.

(3) Knowing the current installation situation (e.g., threat level, CBRN VA, and emergency response capabilities), including the respective organizational commander's intent, commander's critical information requirements (CCIRs), and the commander's CONOPS.

(4) Coordinating with each other to determine if there are any special requirements, including CBRN equipment, operations security (OPSEC) applicable to the mission, arrangements for communications and transportation, credentials for identification, appropriate security clearances or documents, or any peculiar requirements (language, interpreter, customs, etc.) associated with multinational units, if applicable.

(5) Understanding the communications connectivity and software requirements for CBRN warning and reporting.

(6) Becoming familiar with capabilities, the emergency response plan, and SOPs.

(7) Exchanging information on national customs and procedures, if an assignment requires becoming a tenant or transient on an allied HQ installation.

(8) Preparing command-specific capabilities and limitations briefings (including such topics as combat readiness factors, personnel strengths, logistics considerations, and map overlays) for mutual presentation.

b. Installation Coordination With a Tenant or Transient Unit. Upon arrival at an installation, the tenant or transient unit CBRN representative should proceed to the HN OPCEN. Specific coordination measures and information exchange that the installation should provide to the tenant or transient unit may include operational, intelligence, and logistics information (see Figure C-1).

- Reviewing during- and postattack actions, checklists, plans, and concepts, such as—
 - ✓ Postattack reconnaissance.
 - ✓ Installation sector/control zones, boundaries, and transition point locations.
 - ✓ Decontamination points and tenant/transient unit responsibilities.
 - ✓ Contamination avoidance checklist items, such as sheltering locations for equipment.
 - ✓ Contamination control areas and TFAs.
 - ✓ FHP actions (e.g., patient decontamination responsibilities).
 - ✓ Casualty handling.
 - ✓ The processing of contaminated remains and hazardous wastes.
 - ✓ The replacement of personnel.
- Reviewing the implement blackout procedures for areas, sectors, facilities, buildings, airfields, vehicles, flashlights, aircraft, weapons systems, etc.
- Reviewing quarantine, ROM, and isolation plans.
- Planning for the integrated use of CBRN reconnaissance, surveillance, and monitoring assets, to include detectors and detector teams.
- Planning for integrated dispersal or sheltering of critical equipment and vehicles, such as—
 - ✓ Aircraft and weapons systems.
 - ✓ Maintenance equipment.
 - ✓ Fire and crash vehicles and systems.
 - ✓ Base recovery equipment and systems.
 - ✓ Security equipment, vehicles, and systems.
 - ✓ Casualty and patient care medical equipment.
 - ✓ Fuel trucks.
 - ✓ Munitions trailers.
 - ✓ Generators.
 - ✓ Special-purpose vehicles.
 - ✓ CBRN reconnaissance team vehicles.
 - ✓ EOD vehicles.
 - ✓ Ambulances.

Figure C-1. Sample Installation-Level CBRN Coordination With a Tenant or Transient Unit

- Reviewing the plan for Dispersal or sheltering of personnel, to include—
 - ✓ Leadership.
 - ✓ Intelligence support.
 - ✓ Installation recovery teams (EOD, medical, CBRN reconnaissance, damage assessment, etc.).
 - ✓ Security teams.
- Identifying installation actions with respect to dispersal, issue, or shelter-critical supplies, to include—
 - ✓ Food.
 - ✓ Water.
 - ✓ Medicine, CBRN pretreatment drugs, prophylaxis medications, antidotes, and other medical supplies, as directed.
 - ✓ CBRN prophylaxis, as directed.
- Providing information on the installation's exposure control systems.
- Providing guidance on when to administer pretreatments, prophylaxis, and antidotes.
- Providing information on what resources (if available) can be allocated for protecting and hardening CBRN C2 centers, CCAs, and sites where CBRN assets have been dispersed.
- Providing information on the installation's cover, concealment, and deceptions operations, as required, to include—
 - ✓ Smoke and obscuration.
 - ✓ Camouflage netting.
 - ✓ Decoys.
 - ✓ Radar reflectors.
 - ✓ Other systems and methods.

Figure C-1. Sample Installation-Level CBRN Coordination With a Tenant or Transient Unit (continued)

- Allocating resources to support hardening or splinter-protect vital assets using steel bin revetments, sandbags, earth berms, concrete revetments, or other expedient methods, to include—
 - ✓ C4I systems, operations, and centers.
 - ✓ COLPRO facilities.
 - ✓ Utility generation and distribution systems.
 - ✓ War reserve materiel.
 - ✓ POL storage and distribution points.
 - ✓ Munitions storage, assembly, and loading assets and centers.
 - ✓ Supply storage.
 - ✓ Medical facilities.
 - ✓ CCAs.
- Providing assistance, if required, on inspecting all CBRN equipment, such as—
 - ✓ CBRN detection and COLPRO systems.
 - ✓ IPE.
 - ✓ Decontamination.
 - ✓ CCAs and contamination avoidance gear.
- Providing information on the MOPP guidance (e.g., should MOPP gear be immediately available?).
- Briefing units on CCA and casualty collection point locations.
- Briefing units on contaminated waste disposal locations according to applicable environmental considerations and procedures.
- Briefing units on preparing shelters and COLPRO facilities for occupancy and operations.
- Briefing units on reporting shelter status (stocking, number of personnel, and problems) to command centers
- Providing information on duress codes, if applicable.
- Providing guidance on pre-positioning CBRN detection equipment and activating detection systems, such as—
 - ✓ M8 paper on facilities, vehicles, revetments, bunkers, defensive fighting positions, etc.
 - ✓ M9 tape on chemical-protective overgarments.
 - ✓ Detector kits at designated locations (with designated teams).
 - ✓ Other CB detection equipment at designated locations.

Figure C-1. Sample Installation-Level CBRN Coordination With a Tenant or Transient Unit (continued)

- Implementing exposure control systems.
- Identifying CBRN defense required capabilities for assigned missions.
- Preparing sample evacuation plans.
- Exercising contingency plans.
- Determining the locations of all known nuclear facilities and radioisotope resources (e.g., hospitals and clinics with nuclear medicine capabilities and industries with isotopic weld-testing sources).
- Determining the locations of hospitals, clinics, and MTFs.
- Determining what radiation detection equipment is within the AO and to whom it belongs (commercial vendor, government, government agency, or HN).
- Determining the distribution of military radiation measuring instruments to deploying units.
- Determining the disposition of specialized radiation survey teams; identifying the contractual expertise available to negotiate any required civil medical or technical support.
- Determining if friendly or enemy equipment and ammunition containing DU or other radioactive materials are likely to be present.
- Determining the locations and functions of high-priority TIM facilities and associated chemical product lines and storage.
 - ✓ What are the operational levels, security, and infrastructure associated with these TIM facilities.
 - ✓ What storage volumes are associated with these TIM facilities?
 - ✓ What possible or potential environmental contamination exists?
 - ✓ What hydrological, MET, and topographical geospatial data exist for these facilities?
- Determining the local hazard management procedures and identifying civilian agencies responsible for handling incidents.
- Determining what local hazard identification labeling and placarding systems exist.
- Determining the status of the distribution of military CBRN detection equipment to deploying units.
- Determining the disposition of specialized CBRN and TIM reconnaissance teams and equipment.
- Determining the disposition of IPE and CPE.
- Identifying the need for special or modified CBRN or TIM detection equipment or protective equipment.

Figure C-1. Sample Installation-Level CBRN Coordination With a Tenant or Transient Unit (continued)

c. Tenant or Transient Unit Coordination With the Host Installation. Upon arrival at an installation, the tenant or transient unit CBRN representative should proceed to the host installation OPCEN. Specific coordination measures and information exchange that the tenant or transient unit should provide to the installation may include operational, intelligence, and/or logistics information. See Figure C-2.

- Providing information and status on the unit CBRN defense capabilities and functions to include—
 - ✓ Available equipment and supplies that could have a dual-purpose capability (e.g., pumps) and could be used for CBRN defense.
 - ✓ Personnel resources.
 - ✓ Specialist personnel (e.g., CBRN specialists).
 - ✓ Decontamination capability.
 - ✓ CBRN reconnaissance capability.
 - ✓ Biological defense (detection, protection, and decontamination) capabilities.
 - ✓ Medical capabilities (prophylaxis and support).
 - ✓ Engineer capabilities (equipment).
 - ✓ Individual protection capabilities.
 - ✓ Collective protection capabilities.
 - ✓ Fire fighting and specialized emergency support.
 - ✓ Unit mobility status.
- Providing information on the ability of unit communications to integrate with the installation CBRNWRS.
- Providing information on the unit mission and schedule (e.g., how long will the unit be at the host installation).
- Providing information on the unit emergency response plan.
- Providing information on unit POCs and functions.
- Providing information on security capabilities.
- Providing information on mass-casualty management capabilities.
- Providing information on response-time ability (e.g., ability to respond with an emergency team).
- Providing information on the unit's ability to contribute resources to the installation emergency response plan.
- Identifying unique service tactics, techniques or procedures that will require familiarization training for tenant or transient unit personnel from the host installation.

Figure C-2. Tenant or Transient Unit Level CBRN Coordination With an Installation