

## DATA ITEM DESCRIPTION

**Title:** Physical Security Plan for Recovered Chemical Warfare Materiel (RCWM) Project Sites

**Number:** OE-005-17.01

**Approval Date:** 20021001

**AMSC Number:**

**Limitation:**

**DTIC Applicable:** No

**GIDEP Applicable:** No

**Office of Primary Responsibility:** CEHNC-OE-CX

**Applicable Forms:**

**Use/Relationship:** This plan will provide the necessary Physical Security procedures for Interim Holding Facilities (IHF) for Recovered Chemical Warfare Materiel (RCWM) Project Sites. This Data Item Description contains instructions for preparing a Physical Security Plan that outlines security measures for the IHF on RCWM project sites and incorporates guidance from AR 385-61, DA PAM 385-61, AR 190-11, FM 3-19.30, and DOD 6055.9.

### Requirements:

1. The Contractor shall, when required by the Government, submit a Physical Security Plan that describes the security criteria to be employed during RCWM operations, to include storage of RCWM within the IHF.
- 2.0 The Contractor shall prepare a Physical Security Plan using Attachment A to this DID, as an example. Not all paragraphs may be applicable to all project sites.
- 3.0 Attachment B to this DID provides guidance on the performance of a Vulnerability Assessment for the Physical Security Plan.
- 4.0. End of DID OE-005-17.01.

# DID OE-005-17.01

## Attachment A Physical Security Plan

DEPARTMENT OF THE ARMY  
U.S. ARMYCORPS OF ENGINEERS, (District)  
(District Address)

PHYSICAL SECURITY PLAN (U)  
(Project Site)  
(Date)

1. **Mission.** The mission of the (project site name) is to investigate (what are we doing at the project site) and remove any recovered chemical warfare material (RCWM) and contaminated media.

2. **Purpose.** This plan defines the areas of security interest related to (project site location) and specifies the equipment, forces, and devices utilized to protect RCWM and provide an effective security posture.

3. **Objective.**

- a. Prevent unauthorized access to RCWM.
- b. Prevent damage from sabotage, espionage, or unauthorized use of RCWM.
- c. Prevent theft or diversion of RCWM or government equipment and supplies.

4. **Threat Analysis.** Contact with the (insert local/regional physical security office) indicates (no terrorist threat, extreme terrorist threat, whatever the situation is) at this time. The most likely threat comes from (trespassers and other unauthorized attempts or other appropriate terminology) to access the property.

5. **Vulnerabilities.** The following security areas are considered the most vulnerable because of their locations and uses: (Use Attachment 2 for performing Vulnerability Assessments.)

The site (site name) consists of (enter size) and is (fenced or not fenced). This site is where the intrusive investigation will take place. (Depending upon the location of the site, fencing of the entire project site may not be possible.)

The location at (enter name) is the Interim Holding Facility (IHF) where all RCWM will be stored. (The entire area will be surrounded with a fence meeting the minimum requirements (FE-5) as specified in Chapter 5, AR 190-11.) (Possible statements for this section.)

6. **Priorities.** The priority of physical security is:

- a. First to RCWM at the site, then during transportation to the IHF.
- b. Second to the security of equipment and supplies at the (project site location) site due to the sensitive nature of the work and the property.
- c. Third to the security of the equipment and supplies at the (administrative) location.

7. **Limited and Exclusion Areas.** Access to the site (project location) will be controlled by (name of security force) security force. Only those personnel on approved access rosters will be allowed on the site without an escort. The IHF will also be a limited access area. Only personnel from CEHNC, Technical Escort Unit (TEU), and the Edgewood Chemical and Biological Center (ECBC) will be allowed access to the inside of the IHF area once RCWM has been placed in the facility.

# DID OE-005-17.01

## Attachment A Physical Security Plan

### 8. Equipment and Devices to Detect or Delay Intrusion.

a. (Project Site name)

(1) Perimeter boundary: List what, if any equipment or devices are located on the project site, for example: “An FE-5 type fence surrounds the entire site with privacy fencing on 3 of the sides. A video camera is focused on the personnel gate facing the home at the site. This camera is monitored during daylight hours.”

(2) Clear zones: (Does one exist for the project site? May not be necessary for the entire project site.)

(3) Gates: All gates will be locked during the non-operational hours and monitored during operational periods when it is unlocked. The (Security Force) will monitor the vehicle and personnel gate during all hours.

(4) Signs: Metallic Restricted Area signs are used on the fence, one per side (if the project site is fenced).

(5) Inspections and maintenance: The security force checks the fences at the site every (two hours during both operational and non-operational hours - this cyclic rate will be determined based on the threat analysis and if there is RCWM within the IHF). Maintenance of the site is provided by (contractor’s name) through contract with the Huntsville Engineering and Support Center.

(6) When RCWM is secured within the IHF, a 24 hour security guard will be positioned at the IHF.

b. (Secondary location within the project site, if applicable.)

(1) Perimeter boundary: An FE-5 type fence surrounds the IHF.

(2) Clear zones: A 12’ clear zone exists around the IHF (if practicable).

(3) Gates: The gate to the IHF is locked at all times except during transportation of RCWM and when authorized operations are ongoing.

(4) Signs: Metallic Restricted Area signs are used on all four sides of the IHF fence.

(5) Inspections and maintenance: The security force checks the fences at the site every two hours during both operational and non-operational hours.

### 9. Security Lighting.

a. (IHF Location)

(1) Types – Lighting is provided around the IHF.

(2) Types of light source – Per FM 3-19.30, Chapter 5.

(3) Use control and standards: Lighting will remain on at all times when RCWM is placed in the IHF. The control switch for the lighting will be locked to prevent unauthorized access.

(4) Inspections and maintenance: The security force checks the security lighting at the site every two hours during non-operational hours. Maintenance of the site is provided by (USACE District or specified agency).

# DID OE-005-17.01

## Attachment A Physical Security Plan

(5) Emergency actions for power failure: If power failure occurs, Security Forces may be enlarged until the situation is corrected. Generator power will be coordinated by (USACE District or specified agency) in the event the power failure is prolonged.

10. **Communication Systems.** The security force is equipped with both cellular telephones and radios. This provides immediate access to on-call project personnel and to emergency response forces from the (Security Force).

11. **Locks & Keys.** Locks and keys for the IHF gate are controlled by the USACE, and the IHF doors are controlled by TEU, once RCWM is stored within the IHF. Locks and Keys for collateral areas and equipment will be maintained by (specify who). (Use Appendix A for Key and Lock Control Log.)

### 12. **Measures to control Personnel, Vehicles and Material**

a. Personnel Access Controls: Only authorized personnel will be permitted entry into the site or the IHF. Control procedures will assure positive identification of all personnel prior to entry. Visitors and maintenance personnel will be escorted at all times.

b. Escort Requirements: Escorts will keep the visitor under constant observation at all times.

c. Non-operational hours access procedures: The On-site Operations Officer or his designated representative must approve Non-duty hour access. All pertinent facts concerning the access will be recorded and reviewed the by the operations officer.

13. **Personnel Identification System.** Security personnel will check photo identification against the Access Roster prior to admittance to both the site and to the IHF.

14. **Vehicle Control.** Only authorized vehicles are allowed at the site. Only authorized transportation vehicles are allowed in the IHF.

15. **Material Control.** The TEU will manifest all material being transported from the site to the IHF. RCWM will be transported by TEU with an escort.

### 16. **Security Forces.**

a. Type and composition: (Security Force) provides (one or however many is determined to be necessary) security person at the (Project Site) and then an additional security person when RCWM is placed in the IHF.

b. Authority and Jurisdiction: (Name of) District has contracted with the local authorities to provide security at both the project site and the IHF.

c. Weapons, Ammunition, and Equipment: Security personnel are armed and equipped in accordance with standard local procedures.

d. Rules of engagement and use of deadly force: These are commensurate with the rules employed by the local security forces.

e. Training: This is the responsibility of the (Security Force). Site specific instructions have been provided by the on-site Operations Officer and are included in Appendix B.

f. Actions to be taken under adverse weather and limited visibility conditions: Patrols will be maintained during these conditions to ensure security integrity.

**DID OE-005-17.01**

**Attachment A  
Physical Security Plan**

g. Posts: (Explain post locations)

h. Working dogs: (May or may not be applicable)

i. Response force: The (Security Officer) on duty will call for the appropriate response force from the (depends on his assessment of the situation). Response times will be (identify the requirements)

17. **Emergency Actions of General Nature.** Actions pertaining to emergency situations will be in accordance with the (Project Site) Chemical Safety Submission (CSS).

18. **Recovered Chemical Warfare Material Movement.** Procedures for movement of recovered chemical warfare material are as outlined in the CSS.

19. **Coordination.** This plan has been coordinated with all members of the (Project Site) team to include local security, TEU, ECBC, PM Non-stockpile, U.S. Army Engineering and Support Center, Huntsville, and (name of Contractor(s) on site).

20. **Appendices.**

- A. Key and Lock Control Log
- B. Instructions for the Security Force

(Contractor Project Manager's Signature Block)

**DISTRIBUTION:**

Name of Security Force

(Applicable) District, Corps of Engineers, Attention: Project Manager and Security Office

US Army Engineering & Support Center, Huntsville (OE Design Center Point of Contact)

Contractor(s) working the site

Customer's designated representative

CDR, TEU, Attention: (Name)

CDR, ECBC, Attention: (Name)

PM Non-stockpile, Attention: (Name)

**DID OE-005-17.01**

**Attachment A  
Physical Security Plan**

**Appendix A  
Key and Lock Control Log**

Project Site Name: \_\_\_\_\_ Location: \_\_\_\_\_

Lock Number	Where located	Number of Keys	Key Numbers

Date	Key Number	Time Out	Time In	Print Name and Signature

Example (Variations may be used)

**DID OE-005-17.01**

**Attachment A  
Physical Security Plan**

**Appendix B  
Instructions for the Security Force  
(Name of Site)**

Security officers at the excavation site will visually check the site at least once every two hours.

Officers will make radio communication on a periodic basis between posts.

When items are stored at the IHF, officers at the (IHF Location) will station themselves in the vicinity of the IHF to allow maximum observation of the area. Officers will walk around the IHF area at least once every two hours.

In the event an intruder is detected at either site, the officers will take appropriate action to stop the intruder and maintain the security of the site. If necessary, the office will call for appropriate additional support from the (backup security force name). Response times would be in accordance with standard police protocols.

If anything unusual is detected, the officer should contact (name of person the security force should contact) during daytime operations at (phone number). After hours the officer should contact (who) at pager number ( ) or cell phone number ( ).

Questions concerning these instructions should be directed to (name of designated individual).

Enter any additional instructions to the security force.

# DID OE-005-17.01

## Attachment B Vulnerability Assessments

1. A Vulnerability Assessment (VA) will be conducted at each Interim Holding Facility (IHF) to:

a. Determine the facilities vulnerability to sabotage, theft, loss, seizure, or unauthorized access, use of diversion of chemical agents from both external and internal threats.

b. Counter the identified vulnerabilities.

2. Key elements of a VA are identified below:

a. The VA will be accomplished by a team to include the following personnel:

- (1) Project Manager or his designated representative, for FUDS project sites.
- (2) FBI/Military Intelligence office for specific region/site for project site.
- (3) Members of site security forces.
- (4) Local law enforcement personnel.
- (5) Safety and Health representatives.
- (6) Other personnel, as designated by the Project Manager

b. The VA team will be briefed on the purpose and scope of the VA .

c. Briefings will be provided on the storage facility being assessed.

d. Physical Security Plan and SOPS will be reviewed.

e. The VA team will identify specific areas that are of a security interest, target items in the IHF area, and the potential adversary acts for each target.

f. The VA team will tour the IHF site to become familiar with site configuration, terrain, storage structures, security systems and forces, and technical operations. During the tour, the team will identify specific vulnerabilities from internal and external threats to include:

- (1) Observing day and night operations.
- (2) Interview of personnel as appropriate.
- (3) Demonstration of equipment and procedures.
- (4) Note how security systems are utilized, to include forces and backup forces.
- (5) Table-top one or more scenarios to evaluate responses.
- (6) Based on results of scenarios, the team will identify the necessary corrective actions.
- (7) Conclusions and recommendations will be developed and documented by the team. Established vulnerabilities will have specific recommendations for actions to eliminate or reduce the vulnerabilities.

(a) Conclusions will express results that logically flow from the team.

(b) Recommendations will support conclusions.

3. Annotated outline for VA documentations:

a. Introduction

- (1) Purpose
- (2) Scope
- (3) Site description
- (4) Site Mission
- (5) Security Interests

## **DID OE-005-17.01**

### **Attachment B Vulnerability Assessments**

#### b. Identification and Description of Potential Threats

- (1) Insider Adversaries
- (2) Outsider (external) Adversaries
- (3) Insider and Outsider Collusion

#### c. Characterization of Security Systems

- (1) Target Identification
- (2) Identified Vulnerabilities
- (3) Scenarios Developed
- (4) Conclusions and Recommendations
- (5) Team Leader Signature
- (6) MACOM Decisions on Conclusions and Recommendations.

#### **General notes on the VA:**

##### Phase I

1. It is intended to perform the VA in at least two phases, maybe three. The first:

a. Once the team members have been identified, gather all team members to review and assess the following: (Might be done telephonically, once all VA team members have the necessary materials to review.)

- (1) Assess the IHF Siting Plan.
- (2) Face-to-face with local law enforcement to discuss the Physical Security Plan (PSP) for the site.
- (3) Face-to-face with regional FBI or Military Intelligence personnel to discuss the threat situation for the site.
- (4) Review the PSP and other SOPS applicable to Physical Security for the site.
- (5) Review the IHF Plan.

##### Phase II

1. Have the VA Team perform a Site Visit to the IHF, once it is set up. If the location for the IHF is questionable, this Phase may be performed first.

##### Phase III

1. Set up a Table-top exercise; May be run in conjunction with the Table-top for the site operations. Integrate scenarios into the Table-top to incorporate Physical Security into the total picture.