

Guide to
**Managed
Access**

under the
Chemical Weapons Convention

Order No. 122P

Order No. 122P



Distributed by:

Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201
1.800.419.2899
Email: dtirpoutreach@dtra.mil
Web: <http://dtirp.dtra.mil>

June 2004



This pamphlet is part of a series about the Chemical Weapons Convention (CWC) and its potential security impact prepared by the Defense Treaty Inspection Readiness Program (DTIRP) to increase **Readiness Through Awareness** within the United States Government and government contractor community. Additional copies of this pamphlet, as well as other cost-free information about arms control treaties and agreements potentially affecting your facility and related security countermeasures, are also available from DTIRP Outreach Program personnel.

October 30, 1998 (Updated May 19, 2004)

Prepared for:
Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201
1-800-419-2899

From the DTIRP Outreach series: Order No. 122P

TABLE OF CONTENTS

Introduction	2
How to Use this Guide	4
Managed Access: Implied and Explicit.....	5
Object, Purpose, and Means	6
The Verification Annex.....	8
Inspection Mandates	8
Facility Agreements	8
Perimeter Negotiations	9
Pre-Inspection Briefing (PIB)	10
The Inspection Plan	10
Route Planning	11
Specific Measures, Procedures, and Techniques Enumerated in the Convention	11
Remove and Store Sensitive Papers	12
Shrouding	13
Logging Off of Computers.....	13
Presence or Absence Analysis	14
Random Selective Access.....	14
Exceptional Cases	15
The Decision	16
Illustrative Questions and Answers	17
List of Abbreviations.....	20
Related Materials	21

INTRODUCTION

The Chemical Weapons Convention (CWC) is an international arms control treaty prohibiting the development, production, acquisition, stockpiling, transfer, and use of chemical weapons (CW). As a State Party to the Convention, the United States agrees to accept verification measures, including on-site inspections.

The on-site verification measures incorporated in the Convention are the most intrusive of any arms control regime. This is due to both the types of verification activities authorized by the Convention and the large number of facilities subject to these measures. The provision for challenge inspections magnifies this number. A challenge inspection may be carried out at the request of any State Party to the CWC, provided the Executive Council of the Organization for the Prohibition of Chemical Weapons (OPCW) does not reject the request.

In general, the standard for access during the conduct of systematic inspections under the Convention is “unimpeded,” or full and unrestricted, access. For challenge inspections, however, the standard specified by the Convention is “managed,” or limited and/or restricted access. The term

“managed access” was developed to describe the contrasting assumptions and burdens of proof characterizing systematic and challenge inspections. However, the Convention is replete with language limiting or restricting access, even in situations involving systematic or other “routine” inspections. For this reason, access should be viewed as a spectrum or continuum, rather than simply as two disconnected opposites—unimpeded or managed.

As implementers, we must demonstrate compliance with its provisions. In order to do this, while protecting national security, proprietary, and other sensitive information, we must be fully aware of our rights, as well as our obligations under the Convention. A full understanding of the situations in which access may be limited or managed and the means of doing so are an important component of these rights. Understanding managed access is very useful in preparing for any type of CWC inspection, and it is absolutely essential in preparing for a challenge inspection.

The purpose of this guide is to provide a brief reference for further study of this crucial topic. The intended users are site commanders, program managers, site/facility managers, and others involved with inspection preparations.

HOW TO USE THIS GUIDE

This pocket guide is to be used as a supplement to DTIRP pamphlet *Managed Access under the Chemical Weapons Convention* (112P). The sections have been designed to stand alone, in order to facilitate quick reference to the various concepts of managed access.

This pamphlet is not a checklist or a building preparation guide. Instead it is meant to provide the planner and implementer with an understanding of the philosophy and context of the Convention in order to make intelligent choices on managing access.

Text depicted in *italics* throughout this pamphlet are direct quotes from the text of the CWC.

MANAGED ACCESS: IMPLIED AND EXPLICIT

Site commanders, program managers, and site/facility managers with responsibility for treaty implementation planning and preparation are called upon to help demonstrate compliance with the Convention, while simultaneously protecting sensitive information. To address this situation, the Convention's drafters designated managed access as the means for balancing these competing demands. Managed access permeates both the letter and spirit of the CWC verification regime.

The application of managed access is addressed in three ways. First and most generally, the Convention addresses managed access implicitly. The articles state both the object and purpose of the Convention, as well as the means of accomplishing them in rather general terms. In addition, throughout the Convention there are references to procedures to be carried out if agreed. Both the broad language and the requirement that the sides agree on procedures serve to implicitly check an unhindered right of access on the part of the inspection team (IT).

The second kind of reference is the type found in the paragraphs under General Rules in the Verification

Annex or in the Confidentiality Annex. The language there is a bit more explicit. It places obligations on the IT that tend to limit the intrusiveness of the on-site inspection regime and broadly acknowledges the legitimate interests of States Parties to protect critical information and the constitutional rights of their citizens. The provisions on facility agreements between the OPCW and declared facilities are also a clear limitation on access. Through the negotiation of facility agreements this limitation is operationalized.

The third and most explicit way the Convention addresses the access issue is in the paragraphs on managed access in Part X (Challenge Inspections) of the Verification Annex. The Convention provides concrete examples of measures, procedures, and techniques that may be employed in order to protect sensitive information.

OBJECT, PURPOSE, AND MEANS

Article I of the Convention declares each *State Party undertakes never, under any circumstances, to develop, produce, acquire, stockpile, or transfer, directly or indirectly, chemical weapons to anyone*. In addition, *they pledge not to use chemical weapons or encourage or assist anyone to engage in prohibited behavior*. This is the object and purpose of the Convention. The language is important to remember,

even on the operational level. Absent specific CWC provisions, any activity to be undertaken during an inspection by the IT must be satisfactory in the context of these terms of reference. This point may be lost at times, particularly during a challenge inspection.

Article VI affirms each *State Party has the right, subject to the provisions of the Convention, to develop, produce, otherwise acquire, retain, transfer, and use toxic chemicals and their precursors for purposes not prohibited under the Convention*. This is key to understanding the role of declaration verification in inspections and as a limiting factor on inspector activity that should be reflected in the drafting of facility agreements.

Article VIII states the *OPCW shall conduct its verification activities in the least intrusive manner possible consistent with the timely and efficient accomplishment of its objectives. It shall request only the information and data necessary to fulfill its responsibilities under the Convention. It shall take every precaution to protect the confidentiality of information*. The importance of this paragraph cannot be overstated in terms of its ongoing relevance and utility in negotiations during inspections.

THE VERIFICATION ANNEX

Inspection Mandates

Moving from the Articles of the Convention to the Verification Annex, we find more language supporting the application of managed access. The General Rules restate the words of Article VIII in slightly different language, referring to *the least possible inconvenience to the inspected State Party and disturbance to the facility or area inspected*. In addition, *the inspection team shall strictly observe the inspection mandate issued by the Director-General. It shall refrain from going beyond this mandate*. In connection with this clear statement of intent, OPCW IT's have demonstrated a marked commitment to adhering to the letter of their inspection mandates. The mandate, made available before the on-site arrival of the IT, will provide the facility a guide to anticipate potential activities and thereby craft appropriate and legitimate measures to manage access, if necessary.

Facility Agreements

Facility agreements are the basis for inspection activity at chemical weapons, and Schedule 1 and 2 chemical industry facilities. The process of negotiating an individual facility agreement is a means to manage access. Subsequently, whenever an IT proposes activity not covered in the facility

agreement, measures to manage access may be invoked. Schedule 3 and other chemical production facilities will not have facility agreements unless requested by the inspected State Party (ISP) although the inspection procedures are comprehensively stated in the Verification Annex.

Perimeter Negotiations

In challenge inspections, managed access begins with the submission of the requested perimeter. Since inspector right of access to a 50-meter band surrounding the outside of the perimeter lasts for the duration of the inspection, the facility may want to adjust the perimeter outward in the case of undeclared facilities, as the Convention allows. The location of the perimeter on the site may be critical to protecting sensitive areas because activities inside the requested or, if different, final perimeter are subject to managed access.

Even the perimeter negotiations themselves carry, within their CWC-prescribed timelines, an element of managed access. The Convention allows the ISP up to 72 hours after arrival at the inspection site in which to, among other things, negotiate the final perimeter. Additionally, managed access specifically applies to certain exit monitoring procedures, such as inspection of vehicular traffic as well as access to buildings within the 50-meter band.

Pre-Inspection Briefing (PIB)

The Convention requires the presentation of a PIB, lasting no longer than 3 hours, where facility personnel *may indicate to the inspection team equipment, documentation, or areas it considers sensitive and not related to the purpose of the challenge inspection.*

The Inspection Plan

After receipt of the IT's inspection plan, the ISP may suggest changes to the inspection plan, which the Convention states the IT shall take into consideration. This has proven very effective in CWC inspections in the United States. Since no one has better knowledge of a site than the facility management, there is a natural tendency on the part of an IT to accept suggestions, if a logical plan for the inspection can be offered. This is particularly useful to the facility. For example, scheduling access to a given area at a time of day when a sensitive operation or process is not being conducted can effectively protect security concerns while demonstrating compliance. Area and building preparation is made much easier if done on a schedule that is convenient for the facility rather than on a reactive basis.

Route Planning

The ability to plan the physical route (and consequently what the inspectors see and how they see it) is a proactive approach to shaping the inspection plan. This may include roped-off viewing areas or arranged distance viewing. It is important to remember, the "win-win" solution is achievable if the facility and ISP accomplish their task of demonstrating compliance, thereby allowing the IT to do its job.

As an overall synopsis on conducting inspection activities, the General Rules for challenge inspections state: *"The inspected State Party shall provide access within the requested perimeter as well as, if different, the final perimeter. The extent and nature of access to a particular place or places within these perimeters shall be negotiated between the inspection team and the inspected State Party on a managed access basis."*

SPECIFIC MEASURES, PROCEDURES, AND TECHNIQUES ENUMERATED IN THE CONVENTION

Part X of the Verification Annex, and specifically Section C (Managed Access), spells out several measures which *may be employed by the inspected State Party during a challenge inspection to protect*

sensitive installations and prevent disclosure of confidential information and data not related to chemical weapons. These include:

- *removal of sensitive papers from office spaces;*
- *shrouding of sensitive displays, stores, and equipment;*
- *logging off of computer systems and turning off data-indicating devices;*
- *restriction of sample analysis to presence or absence of chemicals listed in Schedules 1, 2 and 3 or appropriate degradation products;*
- *using random selective access techniques...;*
- *in exceptional cases, giving only individual inspectors access to certain parts of the inspected site.*

Remove and Store Sensitive Papers

The inspected facility may remove and store sensitive papers (not related to the compliance concern) from the areas to be inspected. Although inspectors may not open file cabinets or other storage containers, this measure ensures inadvertent access to non-related documents cannot occur. During a challenge inspection, inspectors may request to review documents directly relevant to their inspection mandate and ultimately to the compliance concern. This is quite different from the right of access to records granted the IT in systematic or routine inspections at CW facilities.

Shrouding

Shrouding can be an effective managed access technique when inspectors need to be in an area containing sensitive equipment or other items unrelated to CW and the inspection mandate. Shrouds may be made of virtually any material that effectively conceals the sensitive information. Shrouds may also be used to cover data-indicating devices or displays in sensitive areas of your facility. As an example, it is possible to cover an entire item to obscure its shape, or to cover only a sensitive component such as a gauge or other indicating device.

As in the use of all managed access measures, their employment requires the facility to demonstrate compliance by other means. In the case of shrouding, this may simply mean the partial lifting or removal of shrouding in order to clarify the situation. Facilities should consider this when selecting the material and other characteristics of the shrouding. Additionally, consideration should be given to the fact that shrouding can be costly and may provoke unwanted attention or interest in a particular area, item, or process.

Logging Off of Computers

An effective measure to protect sensitive information may be easily accomplished by logging off of

computers and turning off data-indicating devices, such as monitors or gauges. This is often more practical than shutting down an entire system and is certainly more economical.

When employing this technique, disruption of facility activities can be minimized by instituting a “rolling” preparation procedure where areas and buildings are prepared for inspection on a phased or “just-in-time” basis.

Presence or Absence Analysis

In a challenge inspection, the ISP may apply managed access to the analysis of samples taken within the perimeter. By employing blinding software and removable data storage devices, analysis can be limited to the presence or absence of scheduled chemicals. For example, the United States may limit analysis to detection of a specific Schedule 1, 2, or 3 chemical, their degradation products, or a discrete organic compound identified in advance by the IT. This procedure is useful for the facility because, by analyzing only for a specific chemical, inspectors will not likely gain information about proprietary chemicals or processes used by the facility.

Random Selective Access

In random selective access, inspectors are permitted to select, at their choice, a percentage or sampling of

all of the buildings, areas, or containers to which they seek access. This allows the facility to limit the amount of exposure to areas not related to CW by allowing only a portion of the facility to be inspected. This technique works best when the inspectors are confronted with a large number of similar buildings on a facility, rooms in a building, or containers in a room, area, or vehicle. This last situation—containers in a vehicle—may often arise during exit monitoring at the perimeter. Random selective access can be very useful in this instance, thereby avoiding unnecessary disruption of facility operations.

Exceptional Cases

In exceptional cases, a facility may select individual inspectors for access to a sensitive area. This exceptional access, like all managed access measures, must be negotiated with the IT. Although this measure will probably be more infrequently applied, it can be a useful tool of last resort in order to demonstrate compliance and still minimize access.

When applying managed access, by whatever measures or means, the Convention makes clear the obligation of the ISP to demonstrate compliance by alternate means, if necessary.

THE DECISION

Just as important as understanding the concept of managed access and how it may be applied is knowing if there is a requirement to manage access. This decision begins with an in-depth knowledge of your facility and the larger site, if applicable. A careful self-appraisal of areas, programs, and processes on-site is necessary. While a site commander or facility manager is never relieved of the responsibility to protect national security, there will be, in the case of a challenge inspection, an advance team (AT) and a Host Team formed by the lead U.S. Government agency to lend assistance in preparing to receive the IT on their site. It is crucial for facility management to communicate to the AT and the Host Team any national security and/or proprietary sensitivities on-site as soon as practical after receipt of the inspection notification.

The U.S. Government representatives must also consider any existing inspection precedents that may apply, as well as not setting a precedent unacceptable to another U.S. facility during a future inspection. Consequently, the decision to use or not to use managed access measures is usually made on-site by involving facility managers in coordination with the Host Team. However, there could be a situation where access issues cannot be resolved

during negotiations between the IT and the Host Team and facility managers. If this happens, the issue may be raised through the lead agency to a higher level of the Government.

ILLUSTRATIVE QUESTIONS AND ANSWERS

If, during an initial inspection of a Schedule 2 chemical plant, the IT seeks access to a building on the plant site but not within the declared plant, must full access be granted?

In the absence of a facility agreement, access shall be granted in accordance with the rules of managed access.

During an inspection of a Schedule 3 chemical plant, the IT requests access to plant records. What is the obligation of the ISP?

Although not addressed as managed access, there is a clear difference in the way a records review is handled under the different types of inspections. The relevant paragraph in the General Rules of Verification states: "*Inspectors shall have the right to inspect documentation and records that they deem relevant to the conduct of their mission.*" The relevant paragraph in the Verification Section for Schedule 2

facilities states: “Access to records shall be provided, as appropriate, to provide assurance that there has been no diversion of the declared chemical and that production has been consistent with declarations.”

Finally, the relevant paragraph in the Verification Section for Schedule 3 facilities states: “The inspection team may have access to records in situations in which the inspection team and the inspected State Party agree that such access will assist in achieving the objectives of the inspection.” Implicit in the language governing this inspection activity and especially in the requirement for agreement in the latter instance, is the concept of managed access.

During a challenge inspection at an undeclared facility in the United States, the inspection plan calls for interviews with facility employees. What can be done to manage this activity?

The Host Team and facility managers could set the time and place for such interviews, review the list of potential interviewees for relevance, and have representatives present during the interview. The U.S. Government cannot compel an employee to participate. If the IT and the ISP cannot agree to the suitability of certain questions, the questions will be submitted in written form for reply.

During a challenge inspection, the IT wishes to set up a video camera on the access road in front of the main gate to conduct exit monitoring. Is this allowable?

The CWC provides the right to monitor exit traffic by means of video camera. However, the Verification Annex, in the General Rules, directs the inspectors to employ means causing the least disturbance to the facility and/or area of inspection.

In addition, the same section states the IT should avoid procedures creating a safety hazard; in this case to traffic. It would seem that negotiating the placement of the camera is both legitimate and appropriate.

LIST OF ABBREVIATIONS

AT	Advance Team
CW	Chemical Weapons
CWC	Chemical Weapons Convention
DTIRP	Defense Treaty Inspection Readiness Program
DTRA	Defense Threat Reduction Agency
ISP	Inspected State Party
IT	Inspection Team
OPCW	Organization for the Prohibition of Chemical Weapons
PIB	Pre-Inspection Briefing

RELATED MATERIALS

(order through DTIRP Outreach Program Coordinator at 1-800-419-2899)

101B	Challenge Inspections under the Chemical Weapons Convention
102P	Chemical Weapons Convention—The Impact
104V	Chemical Weapons Convention—The Impact
107V	Managed Access under the Chemical Weapons Convention
108P	CWC—Questions Facing the U.S. Defense Industry
112P	Managed Access under the Chemical Weapons Convention
114P	Features of Chemical Facilities
115P	Routine Inspections under the CWC
117P	Guide for Challenge Inspections under the Chemical Weapons Convention
118P	Guide for Initial and Routine Inspections under the Chemical Weapons Convention
119P	CWC Challenge Inspection Planning Considerations
123A	Development of a Chemical Weapons Convention Pre-Inspection Briefing
125P	CWC Inspection Preparation Guide
127C	Chemical Weapons Agreements Information on CD-ROM
129P	Guide to Scheduled Chemicals

- 131P Rights & Obligations of the Inspection Team & the Inspected State Party under the Chemical Weapons Convention
- 132P Quick Reference Guide to Chemical Equipment
- 133B Role of the Requesting State Party Observer in CWC Challenge Inspection
- 152P CWC Inspector's Privileges and Immunities
- 407C Arms Control Treaties Information on CD-ROM
- 408P Arms Control Agreements Synopses
- 410P Quick Reference Guide to Arms Control Inspection Timelines
- 906B Transparency During Arms Control Inspections
- 907P DTIRP Arms Control Outreach Catalog
- 908V Facility Protection Through Shrouding
- 930C The Arms Control OPSEC Process on CD-ROM
- 936V Verification Provisions—Point and Counterpoint
- 942C DTIRP Outreach Products on CD-ROM
- 950V The Technical Equipment Inspection (TEI) Process
- 951V Arms Control Site Vulnerability Assessments
- 952V Arms Control Security Countermeasures: Selection & Application
- 953V Arms Control Inspection: Site & Building Preparation
- 954T Why TEI?

NOTES

NOTES
