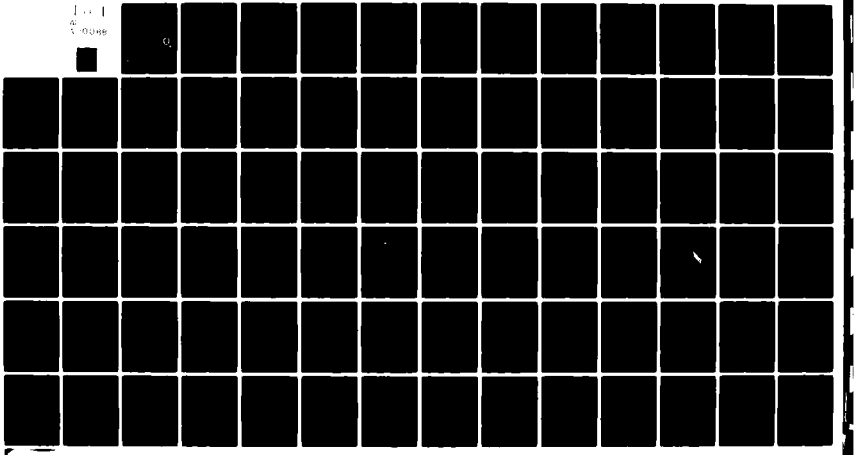
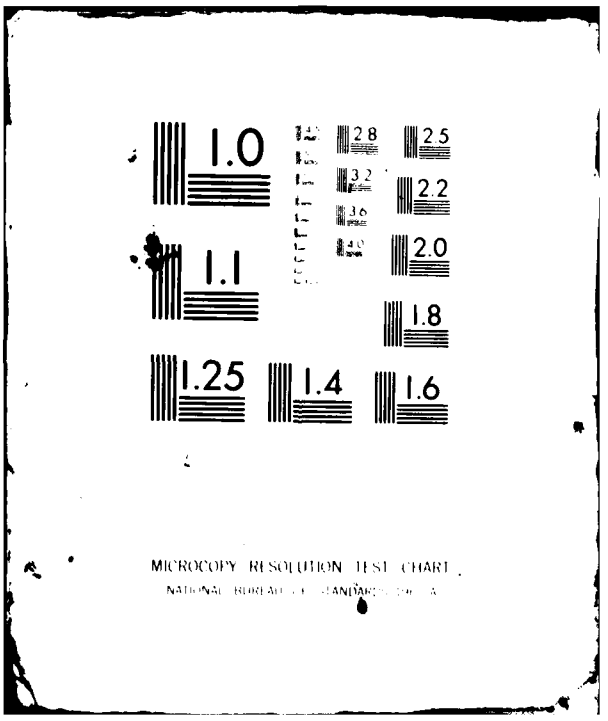
AD-A110 088 BOOZ-ALLEN AND HAMILTON INC BETHESDA MD F/G 15/3
DEVELOPMENT OF SECURITY MEASURES: IMPLEMENTATION INSTRUCTIONS F--ETC(U)
JUL 81 M G OTTEN, D G PIERCE, J E MYRACLE DAAK21-81-C-0024
UNCLASSIFIED HDL-CR-81-024-1 NL



END
DATE FILMED
3-82
DTIC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART

HDL-CR-81-024-1

July 1981

Development of Security Measures: Implementation Instructions for MIL-STD on Physical Security for DCS Facilities

by M.G. Otten
D.G. Pierce
J.E. Myracle

Prepared by
Booz, Allen & Hamilton Inc.
4330 East West Highway
Bethesda, MD 20814

Under contract

DAAK21-81-C-0024

U.S. Army Electronics Research and Development Command
Harry Diamond Laboratories
Adelphi, MD 20783

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER HDL-CR-81-024-1	2. GOVT ACCESSION NO. AD-A110	3. RECIPIENT'S CATALOG NUMBER 088
4. TITLE (and Subtitle) DEVELOPMENT OF SECURITY MEASURES: IMPLEMENTATION INSTRUCTIONS FOR MIL-STD ON PHYSICAL SECURITY FOR DCS FACILITIES.		5. TYPE OF REPORT & PERIOD COVERED Final Report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) M.G. Otten, D.G. Pierce, J.E. Myracle		8. CONTRACT OR GRANT NUMBER(s) DAAK21-81-C-0024
9. PERFORMING ORGANIZATION NAME AND ADDRESS Booz, Allen & Hamilton Inc. 4330 East West Highway Bethesda, Maryland 20814		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Prog. Ele: 33126K MIPR# HC1001040055
11. CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE July 1981 13. NUMBER OF PAGES 76
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

HDL Project: E040E1
PRON: WSO--10401NSA9

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Physical Security	Communications Sites
Sensors	Fences
Military Standard	Barriers
Security Zones	Warning Signs

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The concept of zonal protection for Defense Communications System (DCS) sites was fully developed. The resulting description was formatted according to the requirements for preparing military standards (MIL-STD). The concept description was organized and prepared so that it would readily fit a physical security MIL-STD being prepared by the Defense Communications Agency (DCA) for the protection of DCS sites.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Similarly, line drawings and specifications for physical security measures applicable to the outer two zones of a DCS site were consolidated into a format similar to that for a unit page MIL-STD. User instructions that complement the countermeasure specifications were drafted. These results were formatted to fit the physical security MIL-STD being prepared by DCA.

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturers' or trade names does not constitute an official indorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

per mrs.
nelda mcneal, HDL

A

CONTENTS

FIGURES

APPENDICES

1. INTRODUCTION

1.1 Background

Over the past five years, a number of efforts have been conducted to assess the impact of sabotage on Defense Communications System (DCS) facilities. Some of these efforts have resulted in specific recommendations for implementing security measures to increase the survivability of these assets. However, sabotage, terrorism and vandalism continue to be serious threats to DCS and its ability to provide endurable communications in environments ranging from peacetime to the outbreak of nuclear war. Ensuring DCS' capability to provide communication service in the face of these and other threats has been a major concern of the Defense Communications Agency (DCA).

Existing DCS sites remain highly vulnerable to sabotage because adequate physical security measures have not been implemented. In addition, the future portends even greater problems for DCS as the use of unmanned facilities increases. In order to meet the sabotage threat successfully, concerted efforts are needed to implement adequate physical security measures at existing facilities and to incorporate physical security designs into the plans of future sites.

One factor contributing to the delay in adopting adequate security measures at existing facilities is the lack of a reference standard for evaluating and upgrading security at individual sites for use by commanders and facility operators. Similarly, facility designers do not have a reference for incorporating security into new facility plans. DCA has therefore initiated the development of a physical security military standard (MIL-STD) for protection of DCS assets. This MIL-STD will incorporate design guidelines for implementing security at new and existing sites. In support of the DCA program, Harry Diamond Laboratories (HDL) developed a comprehensive outline of the physical security MIL-STD[1] (presented in Appendix A). Currently, HDL is developing that outline into a complete MIL-STD.

In developing the MIL-STD outline, HDL adopted a zonal approach for allocating physical security. Five zones of protection were defined ranging from zone 0, which encompasses all terrain outside the site perimeter, to zone 4, the innermost zone, which contains all of the critical site elements to be protected (Figure 1).

This report describes the work conducted in support of the HDL program. The overall objective of the work was to provide an in-depth development of selected sections of the physical security MIL-STD. These sections are:

(a) Paragraph 4.3.3.4 Concept of Security Zones

[1] *Booz, Allen & Hamilton Inc., Development of an Outline of a Physical Security Military Standard for Defense Communications System Facilities, for Harry Diamond Laboratories under contract no. DAAK21-80-P-4676 (November 10, 1980).*

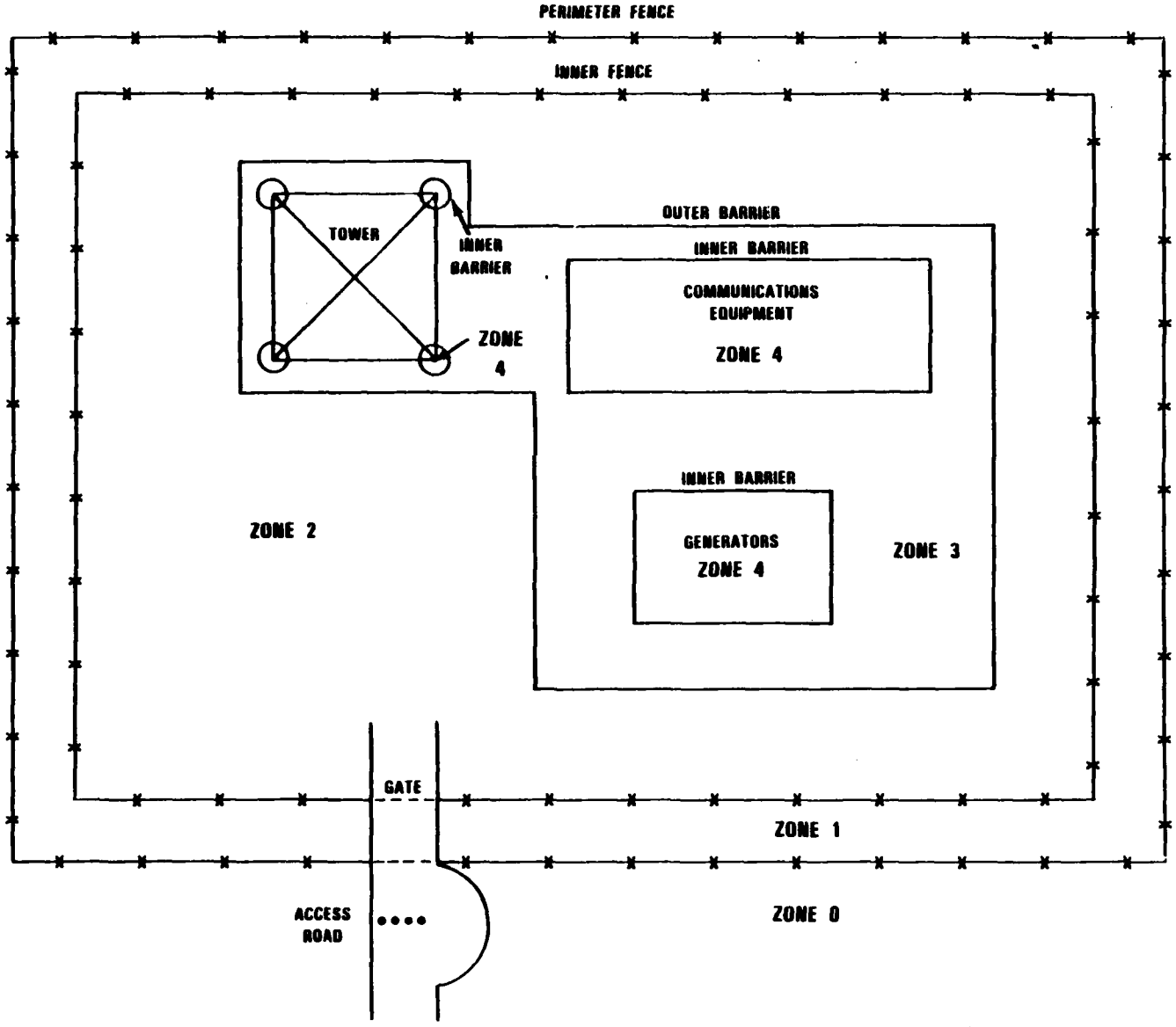


Figure 1. Example of Security Zones for a Generic Unmanned DCS Site.

(b) Paragraph 5.1.3.2 Zone 0 Security Measures

(c) Paragraph 5.1.3.3 Zone 1 Security Measures

1.2 Approach

The general approach used to develop the above paragraphs consisted of the following four efforts:

(a) Pertinent reports, handbooks, regulations, circulars and standards were obtained and categorized into data files to support development of the physical security MIL-STD.

(b) The above data were reviewed to identify concepts of protection similar to those of security zones. Based on the results of this review, the concept of security zones, as applied to DCS sites, was fully defined and formatted to fit paragraph 4.3.3.4 of the MIL-STD.

(c) Physical protection techniques applicable to zones 0 and 1 were identified from sources in the data file. Design and implementation details for those techniques were drafted into a format suitable for use in the MIL-STD.

(d) User instructions were combined with the implementation details described above to develop in detail the full text of paragraphs 5.1.3.2 and 5.1.3.3 of the MIL-STD.

2. DATA COLLECTION

2.1. Data File

After careful survey of existing literature and current government and industry practices, a number of documents relevant to the completion of the selected sections of the physical security MIL-STD were identified. These documents were obtained and organized into a data file. Those references used in developing the selected sections of the MIL-STD are listed in the bibliography of this report. These references are discussed further in the following paragraphs.

2.2 DCA/HDL Efforts in DCS Site Protection

In the 1975-78 time frame, HDL conducted an effort to assess the vulnerability of DCS sites to sabotage.[2,3,4,5] The HDL effort developed and estimated the cost of specific protection approaches to reduce site vulnerabilities. Later, these and other countermeasures were incorporated into a physical security guide[6] for agencies responsible for planning, programming, operating or maintaining DCS assets. However, these guidelines did not present sufficient details to assist existing facility operators or future site designers in implementing the protection techniques.

Careful review of the guidelines led to the selection of many of the protection concepts to be incorporated in the physical security MIL-STD for zones 0 and 1. Design and implementation details for those concepts were then obtained from available physical security documents.

2.3 DCA/HDL Survivability Handbooks

The physical security MIL-STD will be one of a series of handbooks dealing with upgrading DCS survivability in the face of threats ranging from sabotage to nuclear weapon effects. Physical protection concepts were therefore developed to be compatible with concepts that appear in other DCS survivability handbooks to ensure complementary approaches.

---

[2] *Harry A. Gieske et al., Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories, HDL-TM-76-34 (December 1976). (Confidential)*

[3] *Murry B. Ginsberg et al., Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories, HDL-TM-77-19 (October 1977).*

[4] *Murry B. Ginsberg et al., Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories, HDL-TM-78-1 (November 1978). (SECRET)*

[5] *Murry B. Ginsberg, Impact of Sabotage on Manned DCS Facilities: Task II, Harry Diamond Laboratories, HDL-TM-78-13 (November 1978).*

[6] *Defense Communications Agency, Physical Countermeasures for DCS Facilities (Draft), DCA Circular 310-90-1.*

Specifically, the DCA handbook for high-altitude electromagnetic pulse (EMP) protection[7] was reviewed to evaluate the zonal concept used for allocating EMP protection at DCS sites and to ascertain its applicability to allocating physical security measures. Correlations between the two approaches for applying protection were identified. The EMP zonal protection concept was adapted for use in the physical security MIL-STD.

2.4 Military Standard Guidelines

As presented in Section 1 of this report, the overall objective of this effort was to provide an in-depth development of selected sections of the physical security MIL-STD. These sections were developed according to the format requirements specified in MIL-STD-962.[8]

Although MIL-STD 962 establishes the required format of a military standard and the general content of the sections, the specific content of the individual sections is determined only by the requirement that it be complete. However, there are rules that must be followed for diction, punctuation, abbreviations, capitalization, symbols, etc. These rules were applied in developing the physical security MIL-STD sections presented in Appendices B and C.

2.5 Physical Security Documents

During the last 10 years, a large number of physical security documents have been produced. These range from military regulations that establish policies for the protection of Department of Defense assets to physical protection handbooks developed to aid security designers and planners. While very little in the way of new technology has been developed since the earlier DCA/HDL efforts in protecting DCS sites, these documents were useful in developing the selected sections of the physical security MIL-STD.

3. ZONE CONCEPT

3.1 Zonal Approach

The DCA handbook for high-altitude EMP protection introduces the concept of allocating EMP protection at a DCS site using a zonal

---

[7] *Harry Diamond Laboratories, DSN Design Practices for High Altitude Electromagnetic Pulse (HEMP) Protection (Draft), for Defense Communications Agency under MIPR HC1001-9-40086 (30 May 1980).*

[8] *Department of Defense, Outline of Forms and Instructions for the Preparation of Military Standards and Military Handbooks, MIL-STD-962 (22 September 1975).*

approach. This approach consists of separating a facility into several equipotential regions separated by electromagnetic barriers or shields through which EMP energy must pass to reach sensitive electronics. These zone regions and boundaries were delineated on the basis of the practical aspects of the communication facility coupled with equipment and component characteristics. Applying EMP protection consists of providing sufficient levels of shielding at the zonal boundaries to reduce the energy passed to a tolerable level.

The physical security MIL-STD is being developed to be compatible with the above handbook and with other DCA survivability documents. Hence, it was desirable that the MIL-STD incorporate the concept of allocating protection using the zonal approach.

3.2 Data Review

Careful review of the DCA HEMP handbook showed a correlation between the application of EMP protection and physical security protection using the concept of zones. However, the physical locations of these zones are different because of the characteristics of both the threat and the protection techniques used. In fact, the zonal approach used in the HEMP handbook results in the restructuring of zones and their boundaries into functional elements and in the allocation of EMP protection to these elements instead of the zones. These are direct results of the nature of EMP hardening techniques and EMP protection procedures. For physical security, the nature of the protection techniques used is based on the direct application of the concept of zones to the allocation of physical security measures.

Although the concept of security zones is not new, little information was found about the concept during a review of pertinent security manuals. However, the concept of zones is essentially an application of "defense in depth," which is a common approach not only to physical security but also to the deployment of tactical forces for the protection of any asset. The "defense in depth" philosophy is expounded in several of the physical security documents that were reviewed.[9,10] This philosophy was incorporated in the definition of the zonal protection concept for DCS sites.

3.3 Concept Development

Based on the results of the above review, the concept of allocating physical security protection at DCS sites was defined and

---

[9] *U.S. Air Force, Local Ground Defense of U.S. Air Force Bases, Regulation 206-2 (1 August 1974).*

[10] *Sandia Laboratories, Intrusion Detection Systems Handbook, Vol. II, for Department of Energy under contract AT(29-1)789 (November 1976).*

amplified. A concept description was developed and formatted according to MIL-STD-962 requirements. Because of its format, the zone concept description is presented in Appendix B.

Since the concept description was developed for use in the MIL-STD and, hence, for direct use by DCS site commanders and facility operators, it is essentially self-explanatory. The following paragraphs explain some of the rationale associated with its development.

(a) The concept description was written so that the user would clearly understand why the approach is used, where each zone is physically located, where the boundaries are located, and what variations are possible.

(b) In order to maintain continuity with the detailed requirements section of the physical security MIL-STD, it was necessary to structure each site into five security zones, even if sufficient boundaries were not available. The procedure to be used in this case is given in paragraph 4.3.3.4.11 of the concept description.

(c) The expected impacts of the security measures, which will be applied in each zone using the detailed requirements section of the MIL-STD, are presented. Starting with the outermost zone, zone 0, and working in, the concept of protection changes from one of deterrence and detection to one of delay and interception. Hence, the overall protection strategy results in an increasingly stronger physical defense the closer one comes to the component or equipment being protected.

4. SECURITY MEASURES FOR ZONES 0 AND 1

4.1 Objective

The work described herein consisted of developing implementation details and MIL-STD user instructions for physical security measures applicable to zones 0 and 1. The objective of this effort was to consolidate the detailed descriptions in order to draft in detail paragraphs 5.1.3.2 and 5.1.3.3 of the physical security MIL-STD. In addition, the format chosen was selected so that updates and changes to the detailed descriptions could be incorporated without requiring major modifications.

4.2 Summary of Approach

The approach used in this analysis consisted of the following:

(a) Physical protection techniques applicable to zones 0 and 1 were identified after careful review of the results of prior HDL efforts, physical security handbooks, and construction guidelines.

This set of protection approaches included all possible techniques and procedures that could be implemented at both manned and unmanned DCS facilities.

(b) From the above set of countermeasures, an optimum subset was identified on the basis of best engineering judgment and prior experience in the development of protection for DCS sites and other critical assets. Optimum techniques were chosen primarily for their applicability and the practicality of their implementation.

(c) Design and implementation details for those techniques considered optimum were obtained from the handbooks, from commercial vendors, and from interviews with physical security experts.

(d) Details on applicable physical security measures were drafted into a format suitable for use in the MIL-STD. The format chosen for the design and implementation details was similar to that dictated for unit page military standards.

(e) MIL-STD user instructions were drafted to complement the design and implementation details. When coupled with the user instructions, the detailed descriptions completed paragraphs 5.1.3.2 and 5.1.3.3 of the physical security MIL-STD.

4.3 Results

Line drawings and specifications for physical security measures applicable in zones 0 and 1 of a DCS site were consolidated into a standard format for use in the MIL-STD. The format chosen, which is similar to that used for a unit page military standard, consists of the presentation of technical details for implementing each countermeasure in a separate figure in the physical security MIL-STD. These figures cover single or multiple pages depending on the extent of details required. It is expected that each figure in its final form would start on a right-hand page and would consist of an even number of pages (a blank page would be used if necessary). Hence, an entire figure could be replaced in the MIL-STD without interfering with existing text or other figures.

Once the design and implementation details were completed, user instructions were drafted to complete paragraphs 5.1.3.2 and 5.1.3.3 of the MIL-STD. These results are presented in Appendix C of this report. For the most part, these sections are self explanatory. The following paragraphs give some insight into the content of each section.

4.2.1 Zone 0 Security Measures

The techniques described in paragraph 5.1.3.2 would be installed to control and sense vehicular traffic near a DCS site and to enhance visual alarm assessment.

Security measures applied to the access road consist of techniques to keep unauthorized vehicles from approaching a site perimeter and from gaining sufficient momentum to crash through the entrance gate or perimeter fence. A vehicular control gate is specified to prevent sightseeing or casual traffic from entering the access road and tripping the sensor. It is not expected that this gate would stop a determined attacker.

A simple but effective sensor is specified for detecting unauthorized vehicles approaching both manned and unmanned facilities. This sensor would be used in conjunction with the vehicular control gate to screen out casual traffic. The user instructions specify procedures to be taken in the event of an access road sensor alarm. To assist in alarm assessment, the user instructions also specify requirements for eliminating visual obstructions in the immediate vicinity of the site perimeter.

4.2.2 Zone 1 Security Measures

Security measures applied to zone 1 are designed to provide intrusion deterrence and detection and to improve alarm assessment. These techniques are described in paragraph 5.1.3.3 of the MIL-STD.

The MIL-STD details requirements for the perimeter fence that should be used at all DCS sites. Specifications are given for both the construction of a new fence and the upgrading of an existing one. The fence described will prevent the casual intruder from entering a site, but will produce only a minimal delay to the dedicated intruder.

Site entry control procedures are specified for both manned and unmanned facilities. Procedures to be used at unmanned facilities consist of step-by-step instructions to be carried out by personnel requiring access to the site. For manned facilities, instructions are presented to control personnel and vehicular movement through the site entry point.

The MIL-STD details requirements for signs posted on or near the perimeter of manned and unmanned DCS sites. The thrust here is to provide an appropriate warning for deterrence but not to present details concerning the operation of the site or its personnel.

Specifications are presented for maintaining a cleared area within zone 1 to assist in visual assessment of an alarm.

Locks are specified as are key control procedures consisting of step-by-step instructions to be carried out for issuing and maintaining keys.

It was determined during the review of data collected on intrusion sensors that it would be inappropriate in the MIL-STD to specify the use of specific sensors in zone 1. The choice of sensor is extremely site dependent; hence, a sensor that works best at one facility may not be the best at another. The approach taken in the MIL-STD consists of identifying all the factors involved in sensor choice. Once a site commander or facility designer has characterized the site, he would turn to the appropriate military department for assistance in determining the optimum sensor for installation. For exterior sensors, that department is the U.S. Air Force Physical Security Systems Directorate. The MIL-STD presents a rank-ordered list of applicable sensors for zone 1. The ordering presented is based on best engineering judgment in consideration of the diveristy of environments expected at DCS sites. The list includes both commercially developed sensors and sensors under development by the Department of Defense.

Implementation details for the highest ranked four sensors are presented. These details are presented solely to familiarize the user of the MIL-STD with the complexities of these devices. The user instructions specify procedures to be taken in the event of a perimeter sensor alarm.

5. CONCLUSIONS

The concept of zonal protection for DCS sites was fully developed and is presented in Appendix B. This description of the zonal concept has been formatted according to the requirements of MIL-STD-962 and was organized and prepared so that it will readily fit the physical security MIL-STD being developed by DCA. The level of detail presented for the zonal concept is commensurate with that presented in other DCA handbooks on DCS survivability.

Similarly, design and implementation details were developed for security measures applicable to zones 0 and 1 at DCS sites. Detailed user text that complemented the implementation instructions was completed. These details were consolidated into a format suitable for inclusion in the physical security MIL-STD being developed by DCA. The format chosen was selected so that updates and changes to detailed specifications for the security measures could be incorporated without major modifications to the MIL-STD text. The zones 0 and 1 security measures are presented in Appendix C.

The overall objective of the effort was met. The selected sections of the physical security MIL-STD were developed in depth and formatted to readily fit the MIL-STD under development by DCA.

LITERATURE CITED

(1) Booz, Allen & Hamilton Inc., Development of an Outline of a Physical Security Military Standard for Defense Communications System Facilities, for Harry Diamond Laboratories under contract no. DAAK21-79-P-4676 (November 10, 1980).

(2) Harry A. Gieske et al., Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (Confidential).

(3) Murry B. Ginsberg et al., Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977).

(4) Murry B. Ginsberg et al., Impact of Sabotage on Manned DCS Facilities: Task I(U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)

(5) Murry B. Ginsberg, Impact of Sabotage on Manned DCS Facilities: Task II, Harry Diamond Laboratories TM-78-13 (November 1978).

(6) Defense Communications Agency, Physical Countermeasures for DCS Facilities (Draft), DCA Circular 310-90-1.

(7) Harry Diamond Laboratories, DSN Design Practices for High Altitude Electromagnetic Pulse (HEMP) Protection (Draft), for Defense Communications Agency under MIPR HC1001-9-40086 (30 May 1980).

(8) Department of Defense, Outline of Forms and Instructions for the Preparation of Military Standards and Military Handbooks, MIL-STD-962 (22 September 1975).

(9) U.S. Air Force, Local Ground Defense of U.S. Air Force Bases, Regulation 206-2 (1 August 1974).

(10) Sandia Laboratories, Intrusion Detection Systems Handbook, Vol. II, for Department of Energy under contract no. AT(29-1)789 (November 1976).

BIBLIOGRAPHY

Booz, Allen & Hamilton, Development of an Outline of a Physical Security Military Standard for Defense Communication Systems Facilities, for Harry Diamond Laboratories under contract no. DAAK21-80-P-4676 (10 November 1980).

Defense Communications Agency, Physical Countermeasures for DCS Facilities (Draft), DCA Circular 310-90-1.

Department of Defense, Nuclear Weapons Security Manual (U), DOD 5210.41-M (CONFIDENTIAL).

Department of Defense, Outline of Forms and Instructions for the preparation of Military Standards and Military Handbooks, MIL-STD-962 (22 September 1975).

Fite, Robert A., Interim Report Commercial Sensor Evaluation, U.S. Army Mobility Equipment Research and Development Center (7 August 1975).

Gieske, H.A. et al., Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (CONFIDENTIAL) (December 1976).

Ginsberg, M.B. et al., Impact of Sabotage on DCS Facilities: Phase II; Harry Diamond Laboratories TM-78-13 (October 1977).

Ginsberg, M.B. et al., Impact of Sabotage on Manned DCS Facilities, Task I: Survey and Analysis (U), Harry Diamond Laboratories TM-78-1 (SECRET) (November 1978).

Ginsberg, M.B., Impact of Sabotage on Manned DCS Facilities, Task II: Cost-Benefit Analysis, Harry Diamond Laboratories TM-78-13 (November 1978).

Harry Diamond Laboratories, DSN Design Practices for High Altitude Electromagnetic Pulse (HEMP) Protection (Draft), for Defense Communications Agency under MIPR HC1001-9-40086 (30 May 1980).

International Energy Associated Limited, Nuclear Safeguards Technology Handbook, for Sandia Laboratories under contract no. 03-6540 (December 1977).

Johnson, J.D., and Troutman, L.M., Evaluation of Intrusion Detection and Identification System (IDIS), Armament Development and Test Center ADTC-TR-73-102, (November 1973).

The MITRE Corporation, Catalog of Physical Protection Equipment, Books 1-3, Vol. I-VIII, for Nuclear Regulatory Commission, NUREG-0274 (January 1978).

The MITRE Corporation, Guide for the Evaluation of Physical Protection Equipment, Books 1-2, Vol. I-VIII, for Nuclear Regulatory Commission, NUREG-0273 (January 1978)

Robinson, T.S., Evaluation of Security Police Equipment for Air Base Defense, Vol. I, Tactical Air Command Project 74E-020T (May 1975).

Sandia Laboratories, Barrier Technology Handbook, for Department of of Energy (April 1978).

Sandia Laboratories, Intrusion Systems Handbook, Vol. I and II, for Department of Energy under contract no. AT(29-1)789 (November 1976).

U.S. Air Force, Construction Design Criteria for Physical Protection of Air Force Operated DCS Sites, AFCS/DEO (October 1979).

U.S. Air Force, Doctrine and Requirements for Security of Air Force Weapons Systems, AFM201-1 (10 April 1970).

U.S. Air Force, Local Ground Defense of U.S. Air Force Bases, AFR 206-2 (1 August 1974).

U.S. Air Force, Security Police Elements for Contingencies, AFR 125-32 (18 July 1973).

U.S. Air Force, System Security Standard - Command, Control and Communication Systems, AFM 207-21 (April 1973).

U.S. Army, Physical Security, FM19-30 (November 1979).

U.S. Army, The Physical Security Program, AR-190-13 (23 August 1974).

U.S. Navy, Physical Security Manual, OPNAV Instruction 5510.45B (19 April 1971).

APPENDIX A—OUTLINE DRAFT OF A PHYSICAL SECURITY MILITARY STANDARD FOR DCS FACILITIES

1. SCOPE

1.1 Purpose

(Purpose is to prescribe security standards and requirements for new DCS facilities and the retrofit of existing DCS assets.)

1.2 Application

(This standard applies to all government owned, operated and maintained DCS facilities, to all government leased DCS facilities for which the government provides the physical security, and serves as a guideline for other government leased DCS facilities. New facilities shall be designed in accordance with this standard and existing facilities shall be retrofit to meet its requirements.)

1.3 Implementation

1.3.1 Security Program

(A security program shall be developed for each DCS facility according to the standards and requirements detailed herein.)

1.3.2 Applicability

(Each provision of this standard shall be reviewed by the site operating activity to determine the extent of its applicability.)

1.3.3 Compatibility

(The requirements detailed herein shall be compatible with other DCS survivability requirements.)

1.3.4 Conflicting Requirements

(Conflicting requirements that are identified with the application of this standard shall be resolved through the proper chain of command.)

2. REFERENCED DOCUMENTS

2.1 Issues of Documents

2.1.1 Military Specifications

2.1.2 Military Standards

2.1.3 Military Handbooks

2.1.4 Publications

2.2 Other Publications

(intelligence reports)

(construction guides)

(military regulations)

(technical reports/handbooks)

3. DEFINITIONS

3.1 Allocation

3.2 Cold War

3.3 Criticality

3.4 Denial

3.5 Detection

3.6 Deterrence

3.7 Endurability

3.8 Facility

3.9 False Alarm

3.9. False Alarm Rate

3.10 General War

3.11 Hardening

3.12 Intrusion

3.12.1 Deceit

3.12.2 Force

3.12.3 Stealth

3.13 Life Cycle

3.14 Matrix

3.15 Nuisance Alarm

3.16 Operating Activity

3.17 Peacetime

3.18 Real Time Assessment

3.19 Readiness

3.20 Safety

3.21 Security

3.21.1 Guard Force

3.21.2 Physical Security

3.21.3 Procedural Security

3.21.4 Response Force

3.21.5 Security Force

3.21.6 Security Program

3.22 Site

3.22.1 Manned Site

3.22.2 Site Classification

3.22.2.1 Generic Site

3.22.2.2 Unique Site

3.22.3 Unmanned Site

3.23 Survivability

3.24 Threat

3.24.1 Saboteur

3.24.1 Terrorist

3.24.3 Vandal

3.25 Tools

3.26 Vulnerability

3.27 Weapons

3.27.1 Chemical Weapons

3.27.2 Conventional Weapons

3.27.2.1 Explosives

3.27.2.2 Small Arms

3.27.3.3 Stand-off Weapons

3.27.3 Nuclear Weapons

3.28 Zones

4. GENERAL REQUIREMENTS

4.1 Policy

4.1.1 Application

(The requirements detailed herein are mandatory for new construction of DCS facilities and shall be applied to existing DCS sites on a priority basis.)

4.1.2 Priorities

(The operating activities shall establish priorities for the upgrading of existing DCS sites to meet the requirements detailed herein.)

4.1.3 Assessment

(The operating activities shall assess all relevant factors in establishing priorities for implementing the requirements detailed herein.)

4.1.4 Personnel

(The operating activities shall be responsible for the selection and training of personnel to meet the requirements set forth herein.)

4.1.5 Site Size

(Every effort shall be made to reduce the areas encompassed by DCS facilities to eliminate requirements to secure unnecessary terrain but still implement adequate security measures.)

4.1.6 Inspections

(Security measures and procedures shall be inspected regularly to insure compliance with the requirements detailed herein.)

4.1.7 Intelligence

(The operating activity's headquarters shall establish and maintain close liaison with the appropriate intelligence activities to maintain updated threat data for its DCS facilities.)

4.1.3 Foreign National Sovereignty

(The operating activity shall assess the impact of host nation laws and customs on the application of the requirements detailed herein.)

4.2 Security Program Requirements

(The operating activities shall establish security requirements for each individual DCS site.)

4.2.1 Threat Identification

(Based on appropriate intelligence, the operating activity shall establish a threat profile for each individual DCS facility.)

4.2.2 Site Vulnerabilities

(Individual DCS site vulnerabilities shall be identified by the operating activities based on the established threat profile.)

4.2.3 Site Criticality

(The DCA shall establish individual DCS site criticality based on DOD activities served, mission analysis and endurability requirements.)

4.3 User Implementation—General Instructions

4.3.1 Security Program Plan

(The operating activities shall prepare a security program plan for each DCS site that details the implementation of the requirements set forth herein.)

4.3.2 Site Classification

(The operating activities shall determine the classification of individual sites, as set forth herein, for applying the appropriate security measures.)

4.3.3 Security Measures

4.3.3.1 Concept

(The concept of security for DCS sites consists of providing adequate protection to deter intrusions or to delay intruders until an appropriate response force can arrive.)

4.3.3.2 Physical Security Measures

4.3.3.2.1 Passive Measures

(Passive security measures consist of the use of fences, barriers, revetments, walls, and hardening that deter or delay would be intruders.)

4.3.3.2.2 Active Measures

(Active security measures consist of the use of sensors, CCTV, lighting, foams and sprays to detect and assess intrusion, and to provide a measure of non-lethal response to intruders.)

4.3.3.2.3 Reaction Forces

Reaction forces consist of guards, security and response forces whose purpose is to provide a lethal response to intruders.)

4.3.3.3 Procedural Security Measures

(Procedural security measures consist of all human related enhancements to physical security measures such as site entry control, alarm assessment procedures, on-site weapon control, etc., to include the physiological and psychological makeup of guard and response forces.)

4.3.3.4 Concept of Security Zones

(Protection of a DCS site consists of establishing zone boundaries or regions through which an intruder must pass in order to reach his intended target. Security measures shall be applied to each of five distinct zones at each DCS site. See descriptive figure.)

4.3.3.4.1 Zone 0

(Zone 0 encompasses all terrain outside a perimeter fence around a DCS site.)

4.3.3.4.2 Zone 1

(Zone 1 consists of the area between the outer perimeter fence and an inner fence at each DCS site.)

4.3.3.4.3 Zone 2

(Zone 2 consists of the site compound between the inner fence and outer barriers used to protect towers, antennas, power sources and electronic equipment.)

4.3.3.4.4 Zone 3

(Zone 3 consists of the area between outer barriers and inner barriers to potect towers, antennas, power sources and electronic equipment.)

4.3.3.4.5 Zone 4

(Zone 4 comprises the area within the inner barriers which contains towers, antennas, power sources and electronic equipment.)

4.3.4 Security Measure Effectiveness

4.3.4.1 Measures of Effectiveness

(The effectiveness of security measures may be measured in terms of the delay imposed on an intruder and by the added weight penalty imposed on the intruder in terms of tools and weapons required to effect sabotage.)

4.3.4.2 Response Force Time

(Response force time, which is the time required for an adequate force to respond to an intrusion, is measured starting with the first sensor indication of a penetration.)

5. DETAILED REQUIREMENTS

5.1 Security Program Development - Generic Sites

5.1.1 Threat Analysis

(Threats to DCS facilities are identified and categorized.)

5.1.1.1 Threat Categories

(The threat to individual DCS sites can be categorized according to the criteria below.)

5.1.1.1.1 Threat Capabilities

(Threat capabilities range from the casual unaided vandal to a trained, fully equipped team of dedicated attackers.)

5.1.1.1.2 Site Criticality

(The criticality of the site influences the threat resources that would be dedicated to its destruction.)

5.1.1.1.3 Site Location

(The location of a DCS site will affect the level of threat as well as the capabilities required to perpetrate sabotage.)

5.1.1.1.4 Motives

(Threat motives include: vandal - personal material gain or excitement; saboteur - personal grievance or political behavior; demonstrators - protest DCS presence; and agent provocateur - disruption of DCS operations.)

5.1.1.2 Probability of Sabotage Attempt

(The probability of sabotage being attempted against a specific DCS site as determined by the appropriate intelligence activities shall be provided to the operating activity.)

5.1.2 Generic Site Vulnerabilities

5.1.2.1 Threat - Vulnerability Matrix

(A matrix is presented detailing generic DCS site vulnerabilities for the threat categories described above.)

5.1.2.2 Use of Threat-Vulnerability Matrix

(The use of the above matrix to determine specific DCS site vulnerabilities is described.)

5.1.3 Security Measures Implementation - Detailed Instructions

(Security measures to eliminate the vulnerabilities identified above are detailed along with the expected benefit and instructions for their implementation.)

5.1.3.1 Site Selection

5.1.3.2 Zone 0 Security Measures

5.1.3.1.1 Access Road Measures

5.1.3.1.2 Sensors

5.1.3.1.3 Alarm Assessment and Procedures

5.1.3.3 Zone 1 Security Measures

5.1.3.2.1 Perimeter Fence

5.1.3.2.2 Site Entry Control

5.1.3.2.3 Warning Signs

5.1.3.2.4 Tonedown & Camouflage

5.1.3.2.5 Gates and Locks

5.1.3.2.6 Sensors

5.1.3.2.7 Alarm Assessment

5.1.3.4 Zone 2 Security Measures

5.1.3.3.1 Inner Fence

5.1.3.3.2 Sensors

5.1.3.3.3 Alarm Assessment and Procedures

5.1.3.3.4 Non-critical Buildings

5.1.3.3.5 Tonedown and Camouflage

5.1.3.3.6 Fuel Storage Protection

5.1.3.3.7 Lighting

5.1.3.3.8 Antenna Protection

5.1.3.3.9 Waveguide Protection

5.1.3.3.10 Commercial Power Lines Protection

5.1.3.3.11 On-site Guard Force Procedures

5.1.3.5 Zone 3 Security Measures

5.1.3.4.1 Critical Buildings - Barriers

5.1.3.4.2 Tower Barriers

5.1.3.4.3 Foams and Sprays

5.1.3.4.4 Entry Control

5.1.3.4.5 Locks

5.1.3.4.6 Protection for Doors, Windows and Other Openings

5.1.3.4.7 Sensors

5.1.3.4.8 Alarm Assessment and Procedures

5.1.3.6 Zone 4 Security Measures

5.1.3.5.1 Protection of Critical Equipment

5.1.3.5.2 Tower Legs Protection

5.1.3.7 Threat - Vulnerabilities - Security Measures Matrix

(A matrix is presented detailing threat-vulnerability - appropriate security measures.)

5.1.4 Effectiveness of Security Measures

5.1.4.1 Protection - Allocation Matrix

(A matrix is presented categorizing security measures in terms of level of protection afforded.)

5.1.4.2 Use of Protection Allocation Matrix

(The use of the above matrix to determine a desired level of protection is described.)

5.1.4.3 Response Force Characteristics

5.1.4.3.1 Description

(The required characteristics of a response force to prevent sabotage are detailed.)

5.1.4.3.2 Time to Respond

(The time required for a response force to arrive at a site must be less than the penalty imposed by the security measures or they are inadequate.)

5.2 Unique DCS Site Protection

5.2.1 Sites Classified Unique

(The criteria for considering a DCS site as unique are presented along with instructions for modifying the generic site matrices to handle unique site considerations.)

5.2.2 Threat Analysis

(Threats to unique DCS facilities are identified and categorized.)

5.2.3 Unique Site Vulnerabilities

(Unique site vulnerabilities are identified.)

5.2.4 Unique Site Secuitry Measures

(Security meausres to eliminate the vulnerabilities identified above are detailed along with their expected benefit and instructions for their implementation.)

5.2.4.1 Zone 0 Security Measures

5.2.4.2 Zone 1 Security Measures

5.2.4.3 Zone 2 Security Measures

5.2.4.4 Zone 3 Security Measures

5.2.4.5 Zone 4 Security Measures

5.2.5 Example Application of Matrices to Unique Sites

5.3 Security Program Plan

(A formal document that fully describes the planned implementation of the requirements detailed herein shall be developed.)

5.3.1 Operating Activity Responsibilities

(It shall be the responsibility of the operating activity to establish, plan, organize and implement an effective security program at each DCS site.)

5.3.2 DCS Guidelines

5.3.3 Life Cycle Considerations

(The security program plan shall include life cycle considerations.)

5.3.4 Security Program Reviews

(The security program plan shall provide for periodic reviews and inspections to evaluate the overall effectiveness of the security program.)

5.4 Security Measure Effectiveness Tests

(The security program plan shall be audited prior to its implemementation to assure that it meets all requirements set forth herein. In addition, once construction is complete, validation tests shall be conducted to determine the adequacy of the protection implemented.)

5.4.1 Operating Activity Responsibilities

(It shall be the responsibility of the operating activity to organize and implement the security program plan audit and effectiveness tests to validate security measures described above.)

5.4.2 Security Measure Validation Test Plans

(Security measure validation test plans are presented that detail test procedures and instrumentation for collecting appropriate effectiveness data.)

APPENDIX B--A ZONAL CONCEPT FOR THE ALLOCATION OF PHYSICAL SECURITY MEASURES AT DCS SITES

4.3.3.4 Concept of Security Zones. The protection of a DCS site shall consist of implementing security measures, both physical and procedural, within each of 5 separate areas that together encompass the entire site and its immediate surroundings. These areas and their boundaries constitute security zones as defined below.

4.3.3.4.1 Definition. Security zones are continuous regions, delineated by boundaries, that surround the components and equipments to protected. Each site is comprised of 5 security zones (zones 0, 1, 2, 3, and 4). Boundaries between security zones will in most cases consist of barriers that impede the progress of intruders. The actual sizes of security zones are a function of the individual site. Examples of security zones at generic DCS sites are presented in Figures B-1 and B-2.

4.3.3.4.2 Rationale. Security measures are implemented using the concept of security zones to produce a defense-in-depth for the protection of a DCS facility and to facilitate the assessment of security effectiveness by providing well defined zones for the application and evaluation of physical protection.

4.3.3.4.3 Application. Security measures shall be applied to each of 5 security zones resulting in a defense-in-depth consisting of a number of distinct countermeasures that an intruder must defeat in sequence in order to reach his intended target. Defense-in-depth is achieved by siting concentric sensor systems and barriers so that they successfully detect an intrusion and sufficiently delay the intruder so that he can be interdicted by an appropriate response force.

4.3.3.4.4 Impact. Security measures applied to each security zone shall have one or all of the following impacts:

a. Provide intrusion deterrence by producing an obstacle, real or imaginary, to a potential intruder.

b. Increase intrusion delay by increasing the time required by the intruder to penetrate barriers in order to reach his intended target and by burdening the intruder with special or increased equipment needed to penetrate the barrier.

c. Facilitate intrusion detection by providing effective locations for the placement of sensors.

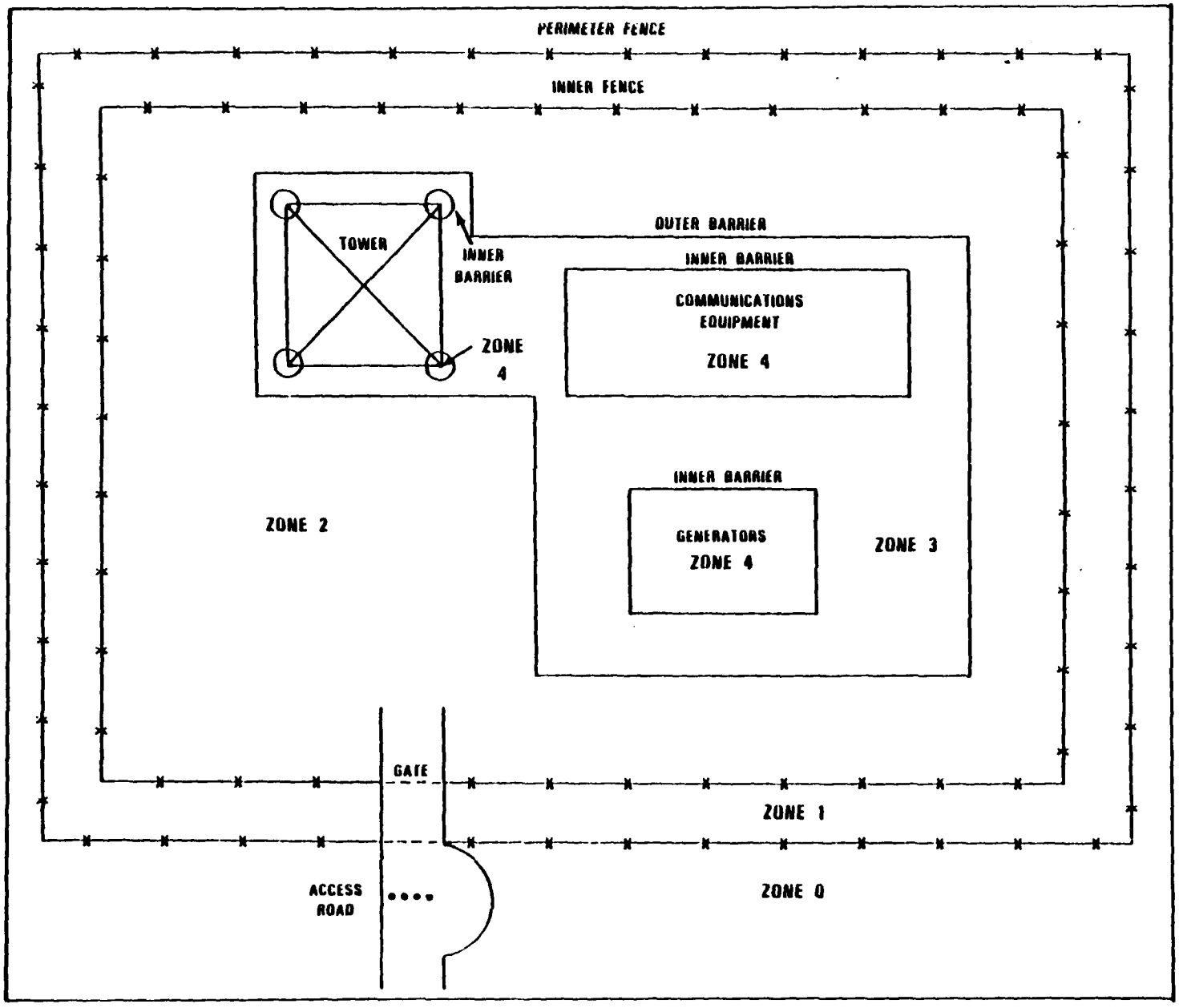


Figure B-1. Example of Security Zones for a Generic Unmanned DCS Site.

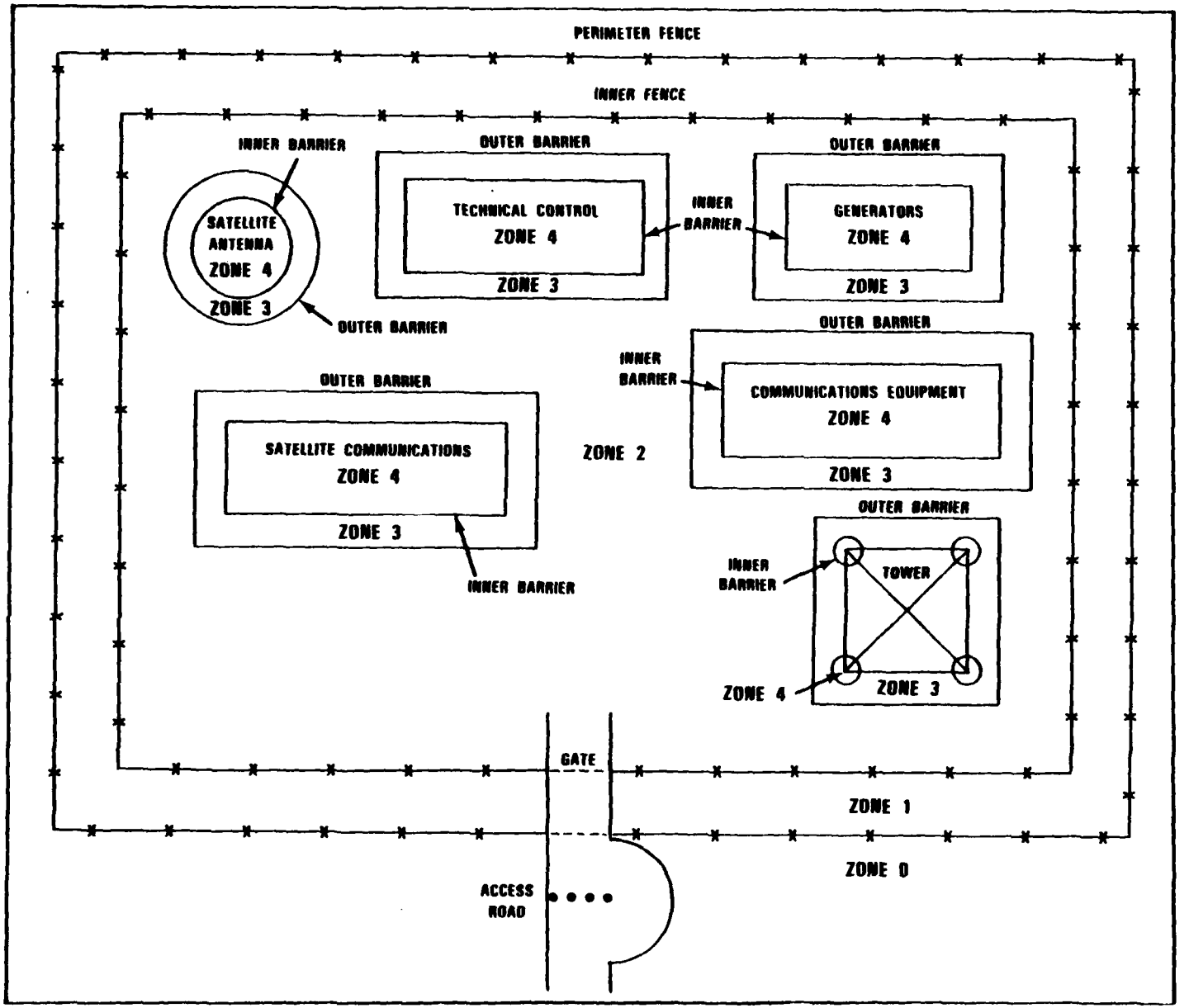


Figure B-2. Example of Security Zones for a Generic Manned DCS Site.

d. Facilitate alarm assessment by providing well defined regions for visual or audio interrogation of sensed intrusions.

e. Enhance effectiveness of security forces by increasing the probability of intrusion detection and by providing sufficient intrusion delay to allow an effective and timely response to an intrusion.

4.3.3.4.5 Characteristics. The following characteristics apply to security zones:

a. Security zones shall be numbered with the highest zone number corresponding to the most secure region of the facility.

b. Each security zone shall consist of a continuous region surrounding the components and equipments to be protected.

c. Adjacent zones shall have zone numbers that differ by not more than one.

d. There may be more than one security zone with the same zone number provided that the preceding condition holds.

e. All sites shall have 5 security zones.

f. The number and location of security zones are independent of the threat.

g. Security barriers consist of security fences, reinforced concrete barriers, walls, domes, and special reinforced concrete or metal sleeves.

h. Security measures applied to security zone boundary openings (gates and doors) shall be commensurate with those applied to the zone boundary.

4.3.3.4.6 Zone 0. Zone 0 consists of the region outside the perimeter fence. Zone 0 typically contains the following site elements:

a. Cleared land outside the perimeter fence.

b. Access road.

c. Parking lots.

d. Commercial power lines.

e. Guy wires.

The primary benefits of security measures installed in zone 0 are improvements in alarm assessment and deterrence and detection of vehicular intrusions. For example, the cleared area outside the perimeter fence facilitates visual assessment of intrusion while a sensored gate in an access road deters and detects vehicle penetration.

4.3.3.4.7 Zone 1. Zone 1 includes the perimeter fence and the region between the perimeter fence and an inner fence. Zone 1 ordinarily contains the following site elements:

a. Perimeter fence, gate, and locks.

b. Cleared area between perimeter and inner fence.

c. Warning signs.

d. Sensors.

The primary benefits of security measures installed in zone 1 are deterrence and detection of intrusions and improved alarm assessment. For example, the perimeter fence deters casual intrusion, a sensor line in the zone 1 cleared area detects fence penetration, and the cleared area facilitates visual assessment of intrusion.

4.3.3.4.8 Zone 2. Zone 2 includes the inner fence, and the area between the inner fence and the outer barriers needed to protect towers, antennas, power sources, and electronic equipment. Zone 2 may contain the following site elements:

a. Inner fence, gates, and locks.

b. Sensors on the inner fence.

c. Perimeter lighting.

d. Closed circuit television.

e. Communication cables.

f. Fuel storage.

g. Fuel lines.

h. Air conditioning.

The primary benefits of security measures installed in zone 2 are intrusion detection and improved alarm assessment. For example, the

sensors on the zone 2 perimeter fence detect intrusion while the zone 2 perimeter lighting and closed circuit television facilitate alarm assessment.

4.3.3.4.9 Zone 3. Zone 3 includes the outer barriers and the area between the outer barriers and the inner barriers needed to protect towers, antennas, power sources, and electronic equipment. Zone 3 ordinarily contains the following site elements:

a. Outer barriers, i.e., walls.

b. Area between the outer barriers and the inner barriers.

c. Waveguides

d. Antennas and antenna feeds.

The primary benefit of security measures installed in zone 3 is intrusion delay to facilitate interception by a reaction force. For example, a reinforced concrete barrier will require added penetration time and require that the intruder carry special penetration equipment such as tools or explosives.

4.3.3.4.10 Zone 4. Zone 4 includes the inner barriers needed to protect towers, antennas, power and fuel sources, and electronic equipment and the area within the inner barriers. Zone 4 may contain the following site elements:

a. Inner barrier.

b. Area within the inner barriers.

c. Towers and tower legs

d. Guy wires and guy wire anchors.

e. Electronic equipment.

f. Power and fuel sources.

The primary benefit of security measures in zone 4 is intrusion delay which allows more time for interception by a reaction force before critical assets are damaged. For example, special concrete sleeves around tower legs will require added penetration time and require that the intruder carry special penetration equipment.

4.3.3.4.11 Variability. Physical barriers should be used to delineate security zones. However, some facilities may not have a sufficient number of physical barriers to delineate 5 zones as defined

above. For example, there may be only one perimeter fence at a site due to inadequate site area. For sites where a sufficient number of barriers cannot be implemented, the 5 zones shall be delineated by barriers and by imaginary boundaries located approximately where the missing barriers would have been placed. The zones shall also be chosen to match the descriptions in 4.3.3.4.6 through 4.3.3.4.10 as closely as possible. Additional physical and procedural security measures shall be implemented on or near the existing barriers commensurate with the levels of deterrence, detection, or delay that would have been provided by the missing barriers. This procedure ensures that all DCS facilities will have 5 security zones for the implementation of physical security measures regardless of the number of physical barriers available. It also ensures that the level of protection afforded a site with an insufficient number of barriers is commensurate with that for a site with physical barriers delineating all 5 zones.

5.1.3.2 Zone 0 Security Measures. Security measures in zone 0 are installed to deter and detect vehicular intrusions and to enhance visual alarm assessment.

5.1.3.2.1 Access Road Security Measures. The number of access roads at DCS facilities shall be kept to the minimum needed for efficient operation of the site.

5.1.3.2.1.1 Access Road. All access roads shall be lined continuously from the nearest adjacent road to the site perimeter fence gate by the vehicle barriers specified in Figure C-1. Vehicle barriers shall not be used along a side of an access road if the terrain immediately adjacent to the road precludes the use of four wheel drive vehicles to circumvent the road. Vehicle barriers shall not be used to line the access road at facilities where the site perimeter is less than 60 m from an adjacent road or where the surrounding terrain offers alternative approaches to the site for four wheel drive vehicles. Vehicle barriers shall be placed as shown in Figure C-1 to prevent straight line approaches by vehicles to the perimeter fence or perimeter fence gate. Vehicle barriers shall be emplaced such that authorized access to a site by emergency or maintenance vehicles is still available.

5.1.3.2.1.2 Parking. Vehicle parking at manned DCS facilities shall be located more than 10 m outside the site perimeter fence. Vehicle barriers as specified in Figure C-1 shall be placed around parking lots to prevent vehicular access to the perimeter fence. No vehicles shall be permitted within the site perimeter fence except those authorized for supply and maintenance purposes. No civilian vehicles shall be permitted within the site perimeter fence.

5.1.3.2.1.3 Entrance. Entrance to site access roads shall be restricted by the use of the vehicular control gate specified in Figure C-2. The vehicular control gate shall be offset a minimum of 10 m from the adjacent road. A vehicular control gate shall not be used at facilities where the site perimeter is less than 60 m from an adjacent road or where the surrounding terrain offers alternative approaches to the site for four wheel drive vehicles. The vehicular control gate at unmanned sites shall remain locked at all times with the following exceptions:

a. If a maintenance crew is on site the gate shall be closed but not locked to allow free passage of emergency vehicles should the need arise.

VEHICLE BARRIERS

Description - Vehicle barriers shall consist of the use of W-beam guard rail supported on S-beam posts to preclude the use of a vehicle in an unauthorized penetration of the site perimeter.

Installation - Vehicle barriers shall be positioned to prevent straight line approaches by vehicles to the perimeter fence and gate (Figures a and b). The vehicle barrier shall consist of galvanized steel W-beam guard rail in accordance with Figure c.

Maintenance - All joints and hardware shall be painted after assembly to prevent rust. Vehicle barriers shall be inspected every 6 months for damage or wear.

References - Location, Selection and Maintenance of Highway Guardrails and Median Barriers, National Cooperative Highway Research Program Reports 54, Southwest Research Institute, San Antonio, Texas, 1968.

Figure C-1. Vehicle Barriers

VEHICLE BARRIERS (Continued)

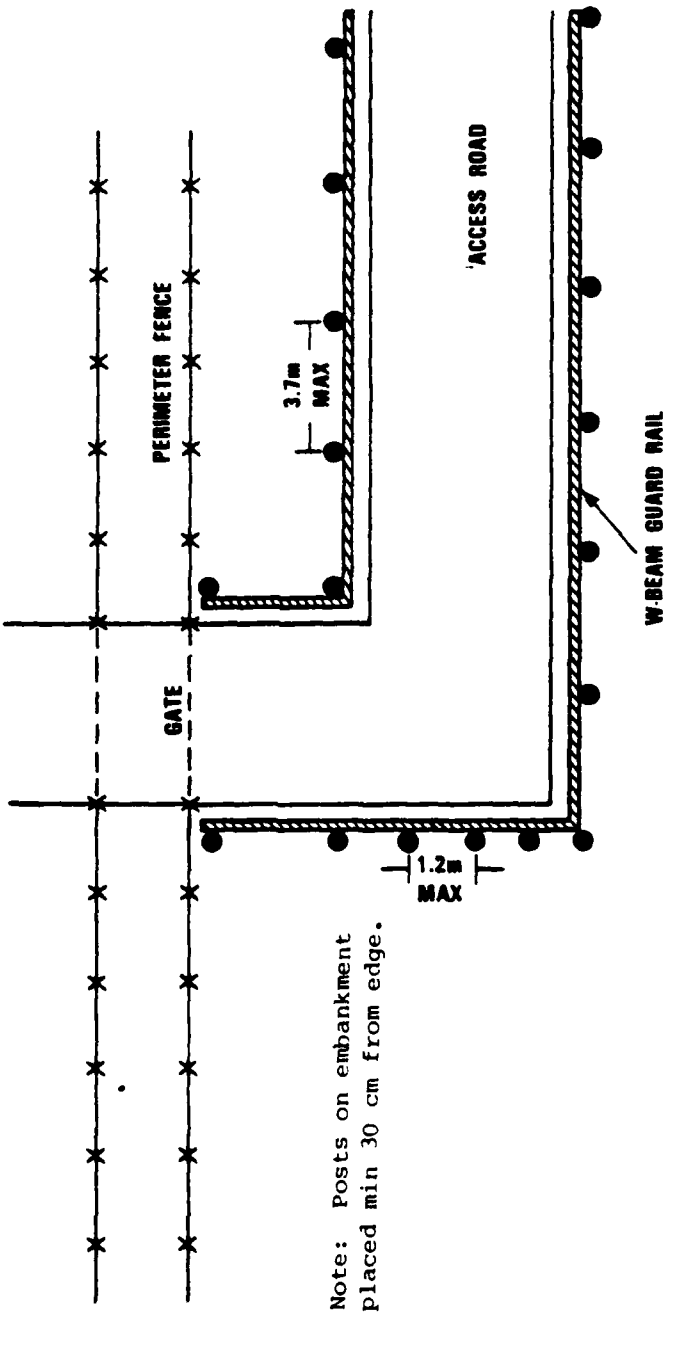


Figure a.

Figure C-1. (Continued)

VEHICLE BARRIERS (Continued)

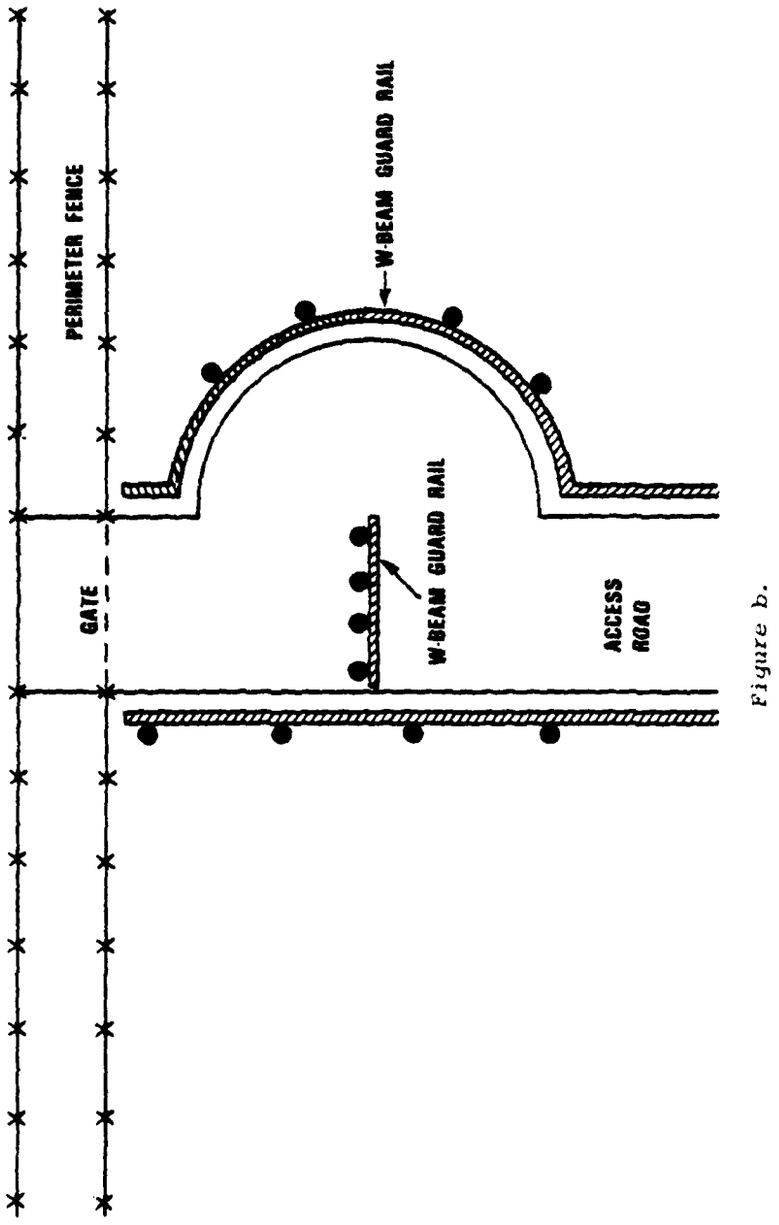


Figure b.

Figure C-1. Continued)

VEHICLE BARRIERS (Continued)

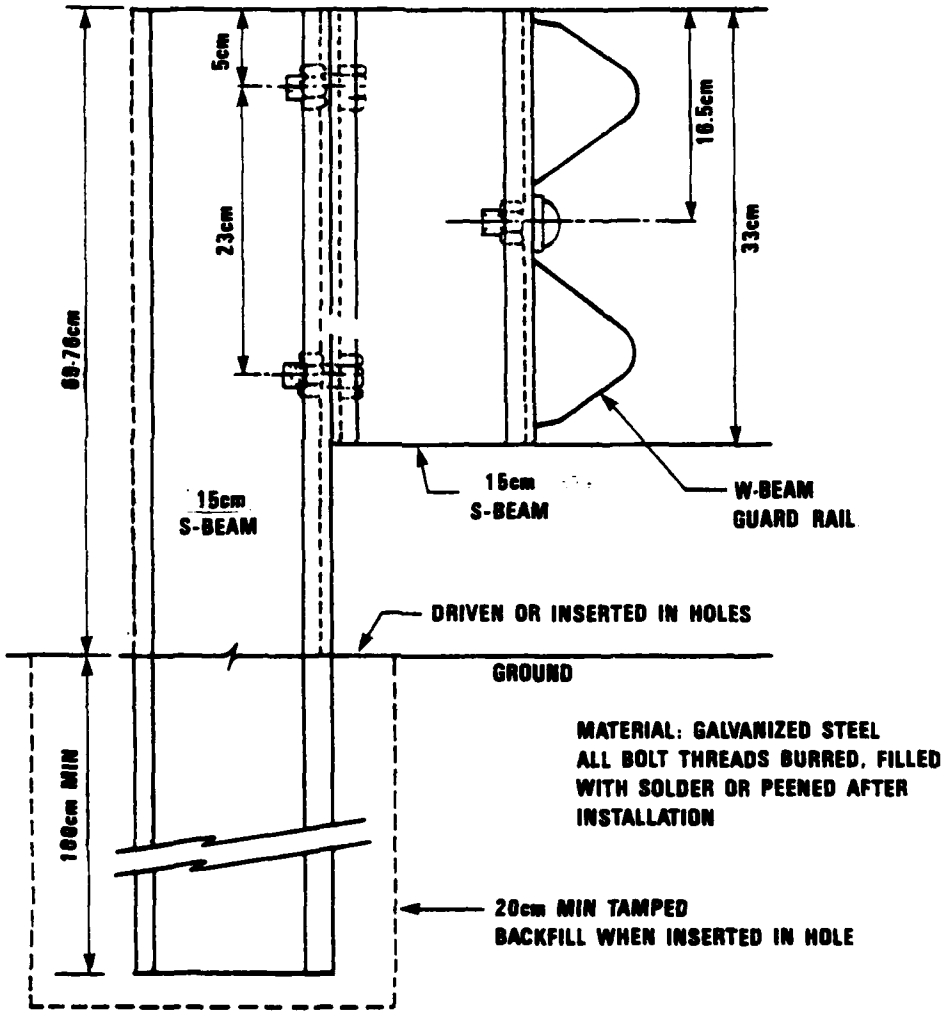


Figure c.

Figure C-1. (Continued)

VEHICULAR CONTROL GATE

Description - A vehicular control gate shall consist of the use of a swingable crash beam supported on posts located near the entrance to the site access road to preclude unauthorized traffic along the access road and to prevent a casual vehicle from being sensed by the access road sensor (Figure a). Vehicle barriers shall be used to prevent a vehicle from circumventing the control gate.

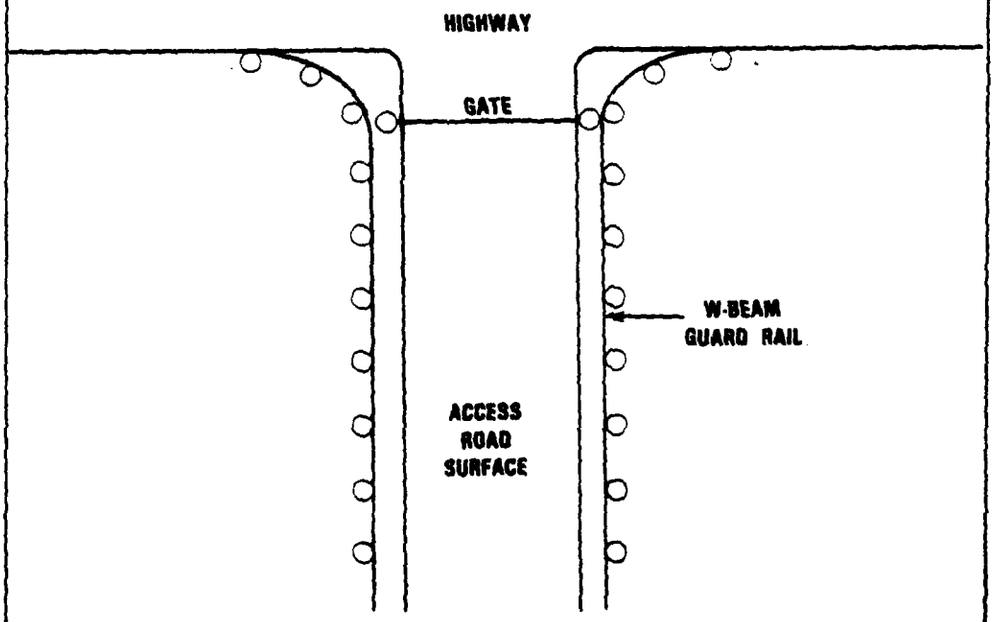


Figure a.

Figure C-2. Vehicular Control Gate

VEHICULAR CONTROL GATE (Continued)

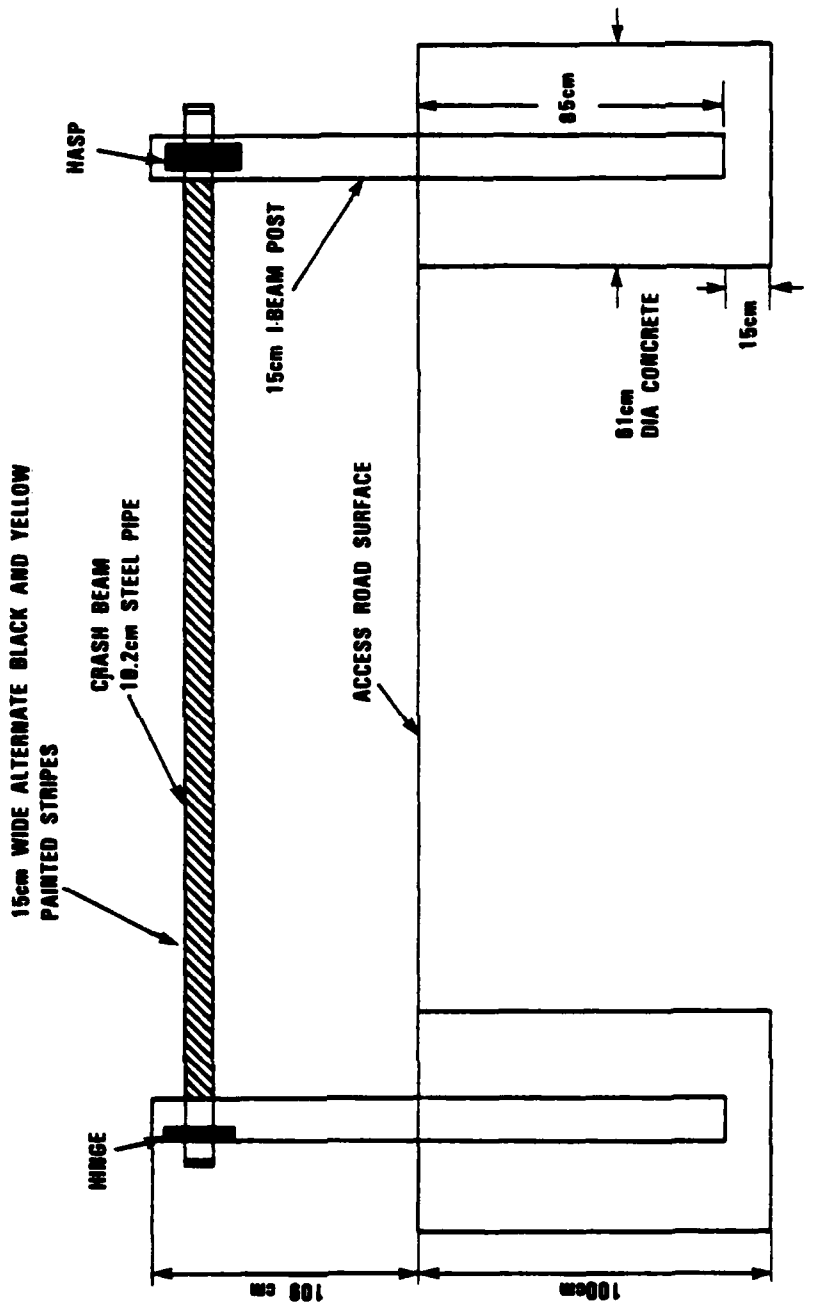


Figure b.

Figure C-2. (Continued)

VEHICULAR CONTROL GATE (Continued)

Installation - The vehicular control gate shall be constructed in accordance with Figure b. The crash beam may be hinged to open vertically or to swing horizontally.

Maintenance - All joints and hardware shall be painted after assembly to prevent rust. The vehicular control gate shall be inspected every 6 months for damage or wear.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

U.S. Army, Office, Chief of Engineers Drawing 40-16-10.

Figure C-2. (Continued)

b. If the first response force to a site intrusion does not have the capability to unlock the gate, the vehicular control gate shall be closed but not locked.

At manned facilities, the vehicular control gate shall be closed except during periods of heavy traffic (for example, shift changes) and during normal visit and delivery times. The vehicular control gate at manned facilities shall not be locked in order to allow free passage of emergency vehicles. The vehicular control gate at both manned and unmanned DCS sites shall be posted with a warning sign as specified in paragraph 5.1.3.3.3.

5.1.3.2.1.4 Entrance Control. Access control for the vehicular control gate shall be accomplished using the site entry control procedures specified in paragraph 5.1.3.3.2.

5.1.3.2.2 Sensors. The access road sensor specified in Figure C-3 shall be employed at all DCS facilities to sense vehicles approaching the site. An access road sensor shall not be used without a vehicular control gate that will preclude sightseeing or casual traffic from tripping the sensor. At unmanned facilities, the sensor output shall trigger an audible alarm on site as well as at the facilities charged with alarm assessments and response force dispatch for the site. At unmanned sites, the sensor shall not be deactivated at any time. At manned facilities, the sensor output shall trigger an audible alarm on site only. The alarm shall not be deactivated unless the vehicular control gate is opened to accommodate heavy traffic (see paragraph 5.1.3.2.1.3).

5.1.3.2.3 Alarm Assessment and Procedures. An alarm triggered by the access road sensor indicates the presence of a vehicle on the access road and inside the closed vehicular control gate. This vehicle presence will be either authorized and hence predicted according to the site entry procedure specified in paragaraph 5.1.3.3.2 or is unauthorized. At unmanned facilities, a response force shall be dispatched upon access road sensor alarm for an unauthorized vehicle's presence. If a maintenance crew is on site, visual assessment may be used to cancel said response action if warranted. At manned facilities, prompt visual assessment of an unauthorized vehicle shall be made, if possible, upon access road sensor alarm. If prompt visual assessment is not possible, for example at a site with a long access road, a response force shall be dispatched upon access road sensor alarm.

5.1.3.2.4 Cleared Area. An extended cleared area of at least 9 m in width shall be maintained, outside the perimeter fence, through the use of chemicals or routine ground maintenance. The cleared area shall not have any obstacles, topographical features or vegetation greater than 20

ACCESS ROAD SENSOR

Description - The access road sensor shall consist of an active loop detector buried in the access roadway as indicated in Figure a. When an approaching vehicle traverses the roadway wire loop, the vehicle's metal changes the industance of the loop, producing an alarm condition.

Installation - The access road sensor wire shall be placed at the bottom of a saw cut (Figure b) and laid in the slot so that there are no kinks or curls, and no straining or stretching of the insulation. All loops shall be wired in the counter-clockwise direction. The wire shall be tamped with a wooden stick in a way that will not cut the wire. Any wire with cuts, breaks, or nicks in the insulation shall be replaced. The wire shall be installed so that each loop is pressed to the bottom of the slot and against one another. Saw cuts shall be made in accordance with Figure c and overlapped so the slot has full depth at all corners. All corners shall be rounded smooth.

Maintenance - Periodic performance testing shall be performed. If the sensor is suspected of degraded performance, testing shall be initiated.

Figure C-3. Access Road Sensor

ACCESS ROAD SENSOR (Continued)

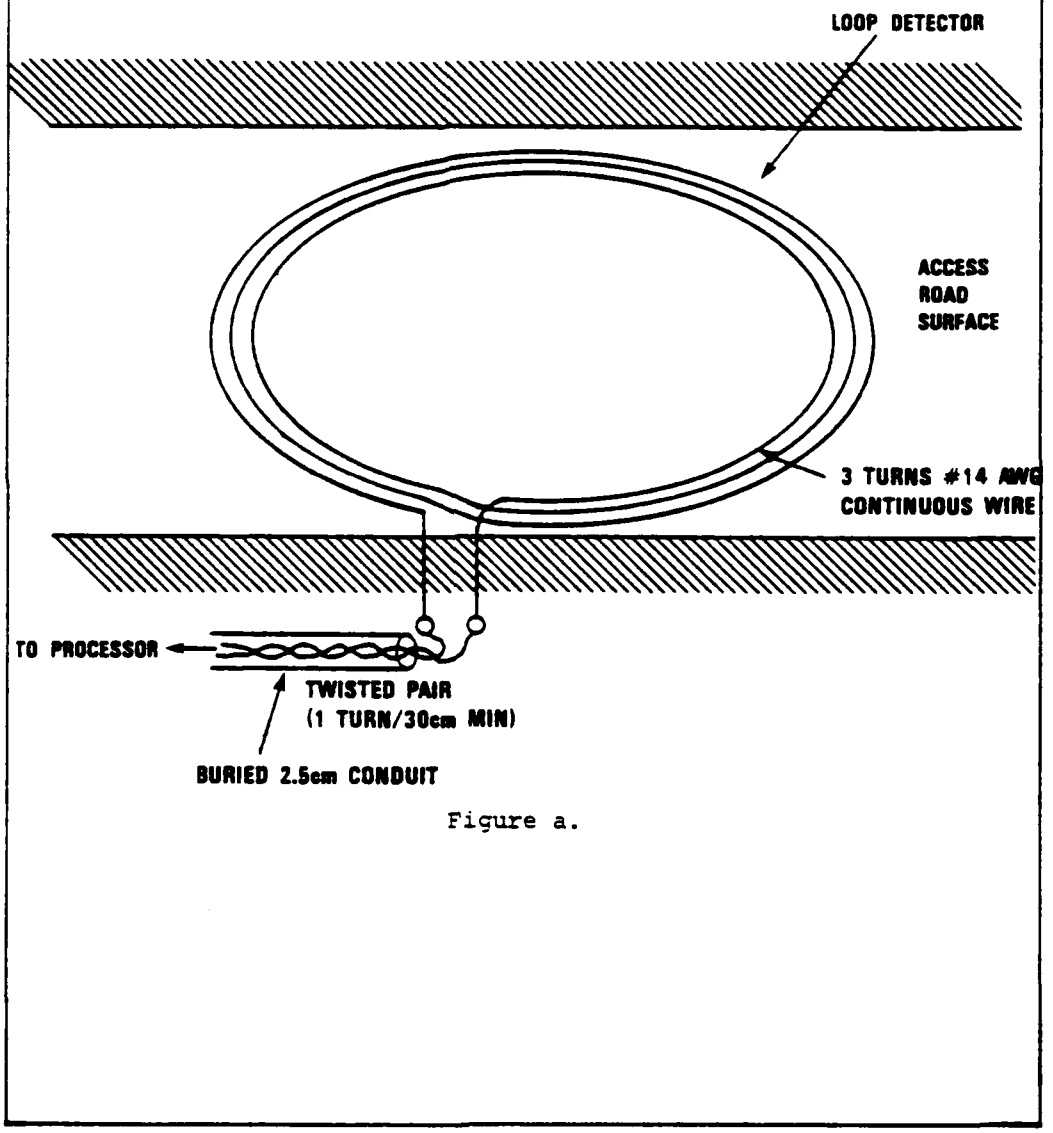


Figure a.

Figure C-3. (Continued)

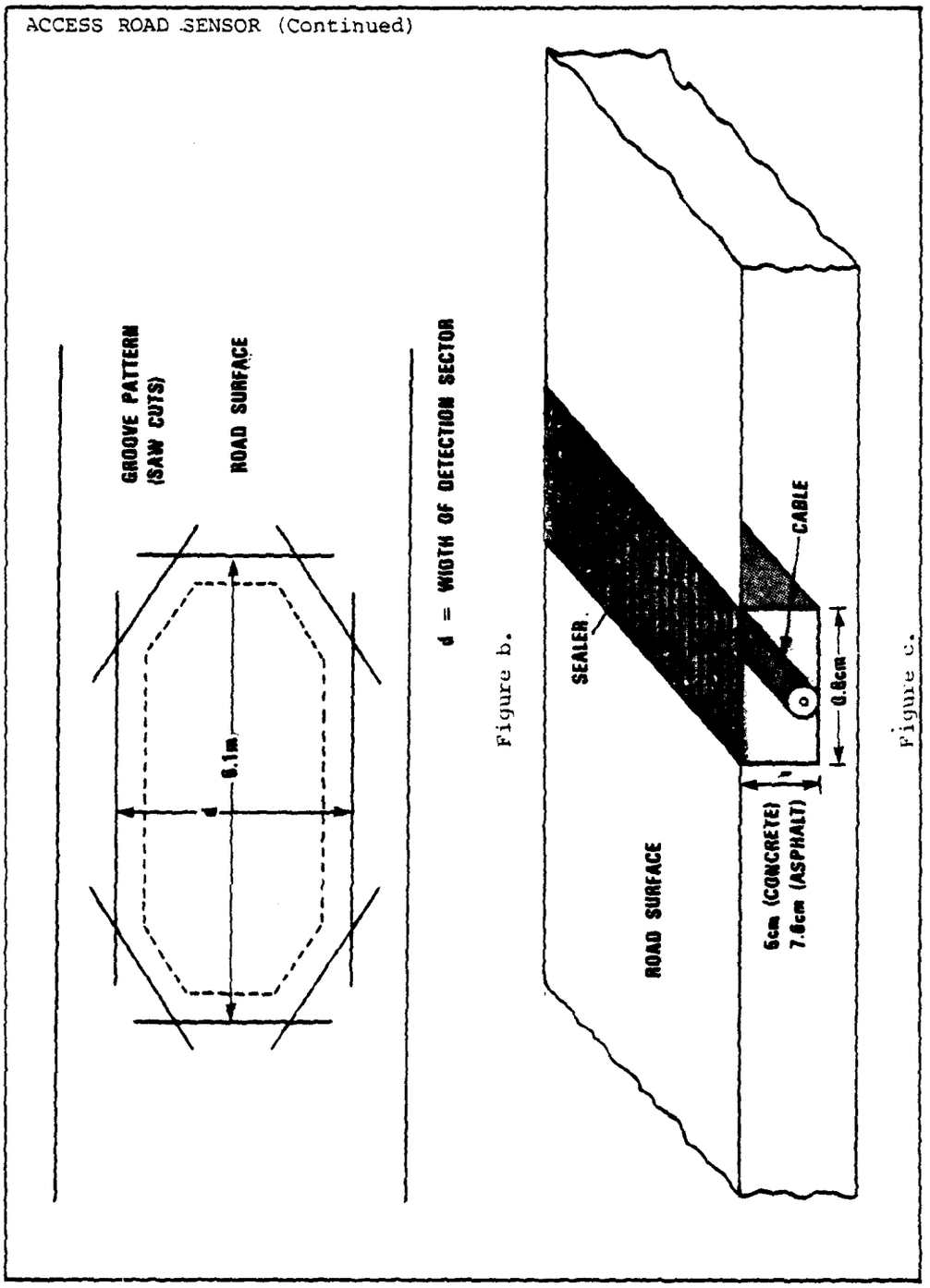


Figure C-3. (Continued)

cm in height. Where possible, topographical features and obstacles shall be removed to permit visual or enhanced visual (binoculars) assessment of access road sensor alarms.

5.1.3.2.5 Cables. All power, communications, and sensor cables entering the site and on-site shall be buried at least 90 cm. The locations of all buried cables shall be obscured. Where practical cables shall enter the site via diverse routes. All manholes and cable vaults on site shall be locked. Off-site, all power cables shall be buried to a distance from the site of at least 600 m. As a minimum, all manholes within that 600 m range shall be locked.

5.1.3.3 Zone 1 Security Measures. Security measures are installed in zone 1 to provide intrusion deterrence and intrusion detection, and to enhance alarm assessment.

5.1.3.3.1 Perimeter Fence. All DCS sites shall be surrounded by a continuous perimeter fence as specified in Figure C-4. New fences shall extend no less than 2.1 meters from the ground to the top of the fence fabric. Existing fences that are at least 1.8 m to the top of the fabric may be modified to the specifications shown in Figure C-4, otherwise existing fences shall be replaced. The perimeter fence shall serve as a legal and physical demarcation of the restricted area boundary. The perimeter fence shall be located no less than 9 m from any facility or equipment critical to the operation of the DCS. The perimeter fence shall be located no less than 3 m from trees, poles, buildings, or other potential climbing aids that are inside the perimeter fence. The distance between the fence and outside trees, poles, buildings, or other potential climbing aids shall be greater than 9 m.

5.1.3.3.1.1 Drainage. Drainage shall be provided to prevent standing water from accumulating near the perimeter fence. All drain lines or culverts extending through the fence lines with cross-sectional area greater than 624 cm^2 and a smallest dimension greater than 16 cm shall be protected by a welded steel grid or replaced by multiple pipes of 25 cm diameter or 619 cm^2 area or less.

5.1.3.3.1.2 Signs. Warning signs as specified in paragraph 5.1.3.3.3 shall be posted at 30 m intervals along the perimeter fence. Warning signs shall be posted also on all gates. Signs shall be posted so that they do not obscure sizable portions of the perimeter fence and approaches thereto.

5.1.3.3.1.3 Gates. Vehicle and personnel gates shall be constructed as specified in Figure C-5. The number of gates shall be kept to the minimum needed for efficient site operation. Only one entry point shall be established and its location shall be based on logical routes of travel into the site. Entry gates shall be positioned parallel to

FENCE

Description - A continuous fence shall be employed around all DCS sites to deter casual intruders.

Installation - Fences shall be constructed in accordance with Figure a, with additional bracing at corners and gates. All posts and bracings shall be mounted inside the fence fabric. The fence shall be topped as indicated in Figure b. Where the fence fabric runs over immovable rock, the fabric shall be positioned within 5 cm of ground level and attached to a 4.1 cm steel bottom rail or taut wire to prevent lifting of the fabric.

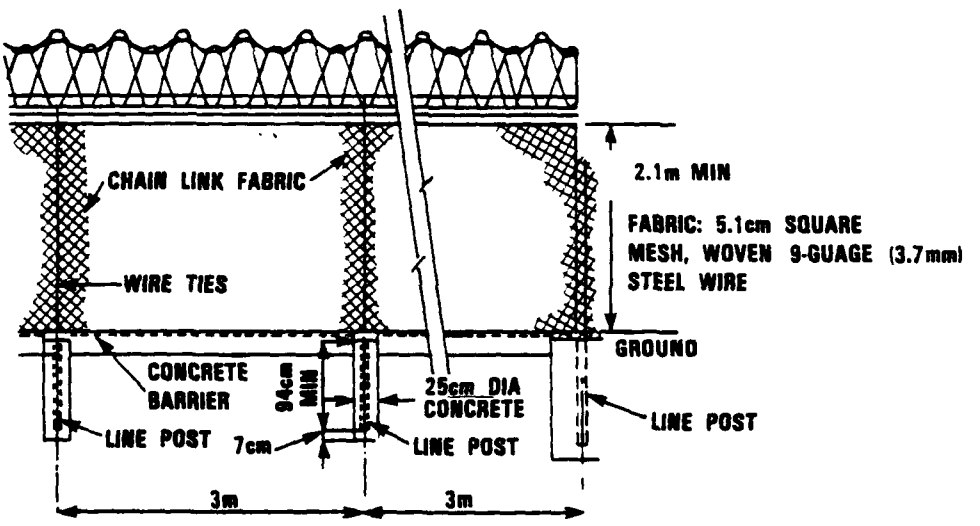


Figure a.

Figure C-4. Fence

FENCE (Continued)

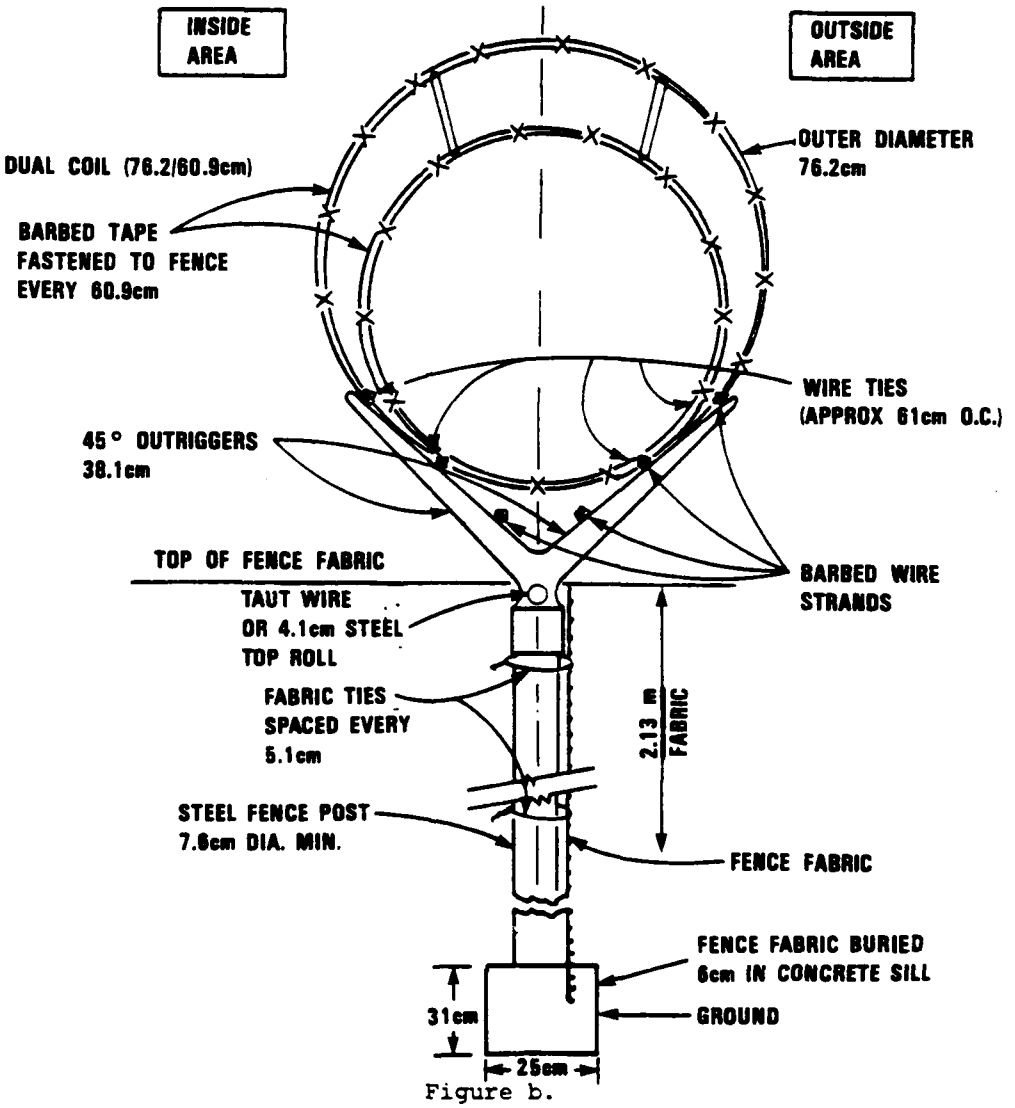


Figure b.

Figure C-4. (Continued)

FENCE (Continued)

Maintenance - Fences shall be inspected daily at manned DCS sites and upon every visit to unmanned sites. Fences shall be inspected for damage, wear or tampering, erosion of soil, loosened fittings or growth of vegetation in the clear areas. Necessary repairs or replacements shall be made as soon as possible. Grid barriers in drainage openings or culverts shall be cleared of debris.

References - Physical Security, U.S. Army Field Manual 19-30, March 1979.

U.S. Army, Office, Chief of Engineers, Drawing 40-16-10.

U.S. Federal Specification RR-R-191/1 Type I.

U.S. Military Federal Specification MIL-B-52775A.

Figure C-4. (Continued)

FENCE GATE

Description - A DCS site shall employ single or double leaf gates on fences for authorized access of personnel and maintenance vehicles.

Installation - Gates shall be constructed in accordance with Figure a. All posts, bracing and hardware shall be mounted inside the gate fabric. All gate hardware shall be peened and welded to prevent removal. Gates shall be topped in the same manner as the adjacent fencing unless that configuration interferes with the operation of the gate in which case a "Y" outrigger may be set at 45 degrees or replaced by a single vertical arm.

Maintenance - Gates shall be inspected daily at manned sites and upon every visit at unmanned sites. Gates shall be inspected for damage, wear and tampering, and loosened fittings. If a gate has been degraded, effectual repairs shall be made as soon as posible.

References - Physical Security, U.S. Army Field Manual 19-30. March 1979.

U.S. Army, Office, Chief of Engineers Drawing 40-16-10.

U.S. Federal Specification RR-R-191/1 Type I.

U.S. Military Federal Specification MIL-B-52775A.

Figure C-5. Fence Gate

FENCE GATE (Continued)

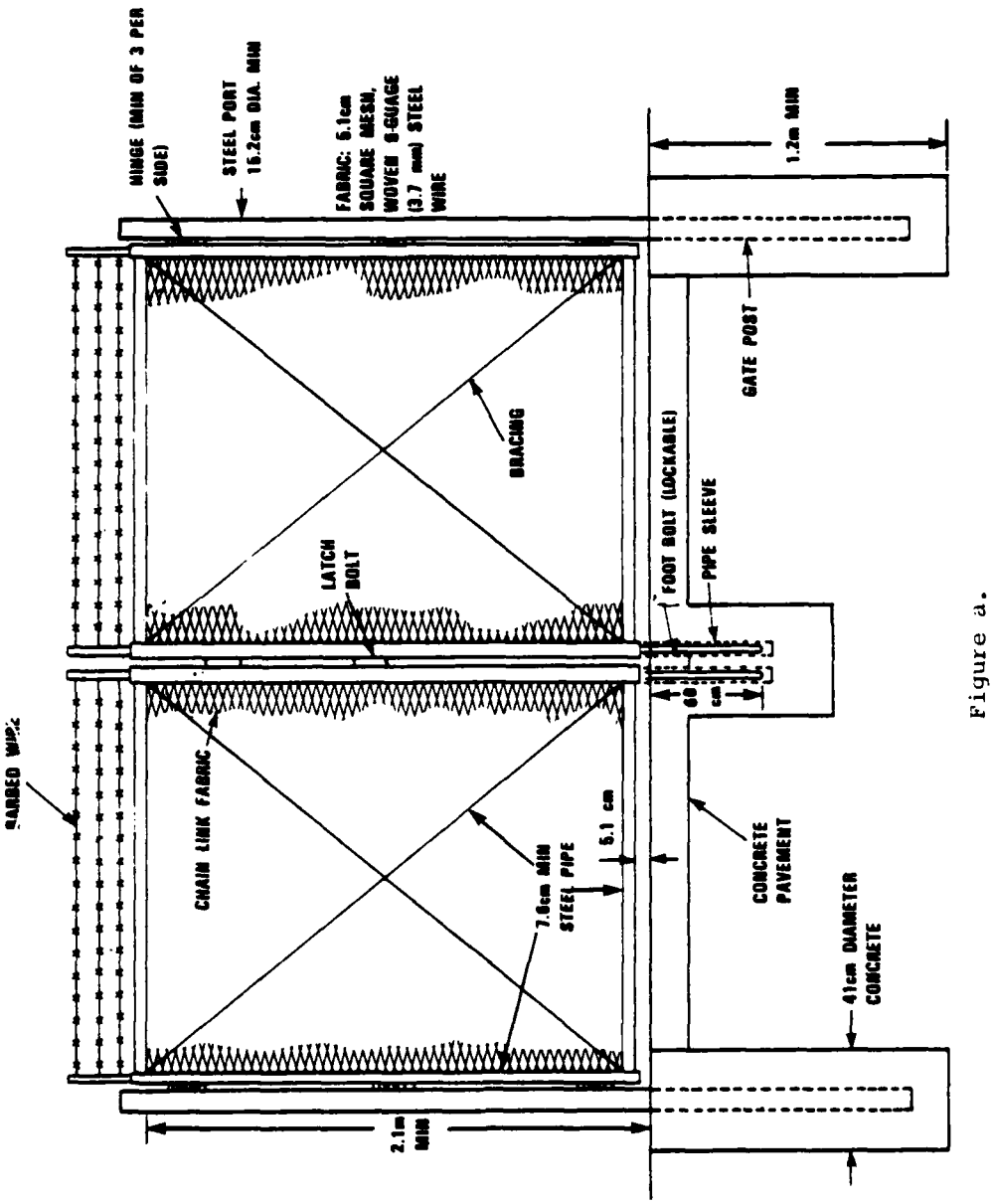


Figure a.

Figure a.

Figure C-5. (Continued)

service or main entry roads. Where entry through a gate is adjacent to heavily traveled roads, the gate shall be offset a minimum of 6 m from the edge of the road for vehicle safely. Gates not under security force observation shall be securable to the strength of the adjacent fence construction. Such gates shall be locked.

5.1.3.3.1.4 Entrance. Vehicle and personnel gates shall be secured with high security padlocks (see paragraph 5.1.3.3.5). At unmanned facilities, gates shall be locked at all times, even when maintenance personnel are on site. At manned facilities gates shall be locked at all times except during times of heavy traffic through the gate (for example, shift changes) at which time, an onsite guard shall be posted at the gate.

5.1.3.3.1.5 Entrance Control. Access control for the vehicle and personnel gates shall be accomplished using the site entry control procedures specified in paragraph 5.1.3.3.2.

5.1.3.3.1.6 Entry Point Lighting. Entry point lighting shall be used at manned facilities for which entry controls are required during normal operations. Entry point lighting shall facilitate accurate and rapid identification of personnel requiring entry into the site. Two or more light fixtures shall be placed such that the light sources are above and behind the entry controller and face the person approaching the site. The intensity of the entry point lighting shall be not less than 16 lux for a distance no less than 15 m outward from the entry point.

5.1.3.3.2 Site Entry Control. Site entry control procedures shall be established to facilitate control of entry and exit of personnel and vehicles for both manned and unmanned DCS facilities according to the guidelines presented in paragraphs 5.1.3.3.2.1 and 5.1.3.3.2.2. Only authorized and essential personnel shall be allowed access to DCS sites. Authorization requirements shall be established according to the needs of the individual DCS site (for example, security clearances). At no time shall an unauthorized individual be allowed access to any DCS site without continual escort by personnel empowered by the site commander to authorize the entry of said individual.

5.1.3.3.2.1 Unmanned Site. Entry control at an unmanned DCS site shall be accomplished by adopting a set of procedural guidelines with an overall objective of verifying the authority of each person seeking entry to a site. These guidelines shall consist of step-by-step instructions to be carried out by personnel requiring access to the site. As a minimum, these guidelines shall include the following steps:

a. Log books shall be established and maintained to record pertinent information regarding each site entry (for example, names of individuals, vehicle used, estimated and actual time in, time out, purpose of visit). Log books shall be kept at the

facility charged with operation and maintenance responsibility of the unmanned DCS site and at the facility charged with dispatching a response force on sensor alarm. Log book entries shall be completed prior to and following each visit.

b. An estimated time of arrival on site shall be established for each visit and shall be adhered to as closely as possible. Alarms triggered by an authorized entry shall correlate with estimated time of arrival for logged site visits.

c. Upon access to a site, all gates shall be closed and locked according to the requirements specified in paragraphs 5.1.3.2.1.3 and 5.1.3.3.1.3.

d. Upon access, telephone contact shall be made with the facility charged with dispatching a response force on sensor alarms and with the facility charged with operating and maintenance responsibility. A prearranged code word or signal shall be passed to assure personnel are not being held hostage.

e. Upon exit, telephone contact shall be made with the facility charged with dispatching a response force and with the facility charged with operation and maintenance responsibility. All gates shall be locked after passage.

5.1.3.3.2.2 Manned Sites. Entry control at a manned DCS site shall be accomplished by adopting a set of procedural guidelines with the overall objective of verifying the authority of each person seeking entry to the site. These guidelines shall consist of step-by-step instructions for personnel and vehicle movement control. As a minimum, these guidelines shall include the following steps:

a. Access lists shall be established to identify personnel who have authorized and valid access rights commensurate with the security clearance requirements of the site. Access to a DCS site shall be limited to only those on the access list. Personnel not listed, who have a valid need for site access, shall be escorted at all times. On-site guards shall not be used for escort.

b. A procedure shall be established for positive identification of persons authorized access to the site. This procedure shall consist of the use of security identification cards and badges. However, for small sites, personal recognition may be used.

c. If an on-site guard is posted at a entry gate, said guard shall make visual assessments of all personnel requesting entry to the site. The guard shall have available to him a fixed or portable duress alarm.

d. For sites where an on-site guard is not posted at an entry gate for 24 hours a day, a call box or intercom shall be maintained at the perimeter fence gate. A closed circuit T.V. system shall be erected to allow remote assessment of personnel requesting access. A fixed duress alarm shall be positioned near the CCTV screen.

e. Only authorized and official vehicles shall be allowed on site. Personnel parking shall be maintained outside the perimeter fence according to the requirements specified in paragraph 5.1.3.2.1.2.

5.1.3.3.2.3 Emergency Entry. In an emergency, firefighting, medical or other required emergency personnel shall be permitted entry to a site without delay. Said emergency personnel shall be kept under escort and surveillance by site operational or security personnel at all times and shall be restricted to the area containing the emergency situation.

5.1.3.3.3 Warning Signs. Restricted area signs shall be posted on all sites subject to the jurisdiction or administration of, or in the custody of the DOD or military departments of the DOD according to the requirements of DOD Directive 5200.8 and Section 21 of the Internal Security Act of 1950. Any posted sign shall not reveal the nature of the operation of the site and shall not present information about site personnel. Specific wording on signs shall be consistent with host nation requirements and posted in both English and local languages. Specifications for signs are presented in Figure C-6. An example of a restricted area sign is also presented.

5.1.3.3.4 Cleared Area. An extended clear area of at least 9 m in width shall be maintained inside the perimeter fence through the use of chemicals or by routine ground maintenance. The cleared area shall have no obstacles, topographical features or vegetation greater than 20 cm in height.

5.1.3.3.5 Locks and Keys. All gates, manholes, cable vaults and doors shall be locked with high security key operated padlocks that meet or exceed the requirements of MIL-P-43607E. Key control procedures shall be adopted that consist of step-by-step instructions to be carried out for issuing and maintaining keys. As a minimum, these instructions shall include the following steps:

a. A key control officer shall be appointed to have overall responsibility for issuance and maintenance of keys and locks.

b. Keys shall be accessible only to those persons whose official duties require access to them. A record shall be kept of the total number of keys and the names of persons to whom keys have been issued.

WARNING SIGNS

Description - Warning signs shall be employed at all DCS sites to deter casual intruders. The sign illustrated in Figure a is for example only. The format and content used for a sign will be a function of the location of the site and the applicable U.S. and foreign regulations.

Installation - Signs shall be made in accordance with Figure a. Warning signs shall be printed in English and the local language. The sign shall be painted white. The word WARNING shall be bright red in color. All remaining letters shall be black.

Maintenance - Warning signs shall be inspected daily at manned DCS sites and upon every visit at unmanned sites. Signs shall be inspected for damage, wear and tampering. If warning signs

Figure C-6. Warning Signs

WARNING SIGNS (Continued)

have been degraded, repairs or replacements shall be made as soon as possible.

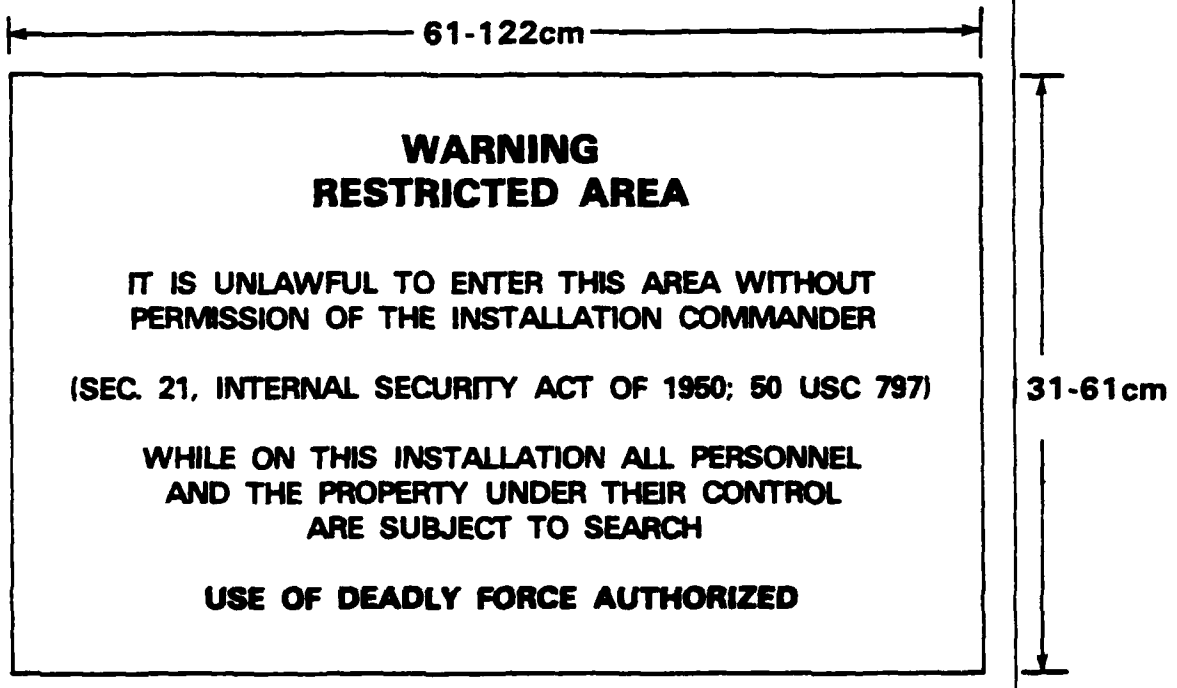


Figure a.

Note: Reflective lettering
3.7 cm min. height.

References - Doctrine and Requirements for Security of Air Force Weapon Systems, U.S. Air Force Manual 207-1, 10 April 1970.

United States Navy Physical Security Manual, OPNAV Instruction 5510.45B, 19 April 1971.

Physical Security, U.S. Army Field Manual 19-30, March 1979.

Figure C-6. (Continued)

c. Padlocks shall be changed on a regular basis and upon possible compromise of a key.

d. Keys shall be stored in a locked container when not in use. Access lists for those authorized to draw keys shall be kept in the same container.

e. Keys shall not be issued for personal retention.

5.1.3.3.6 Sensors. One or more intrusion sensors shall be installed within zone 1 for the purpose of detecting unauthorized penetrations into manned and unmanned facilities. Sensors shall be installed within the perimeter fence. For unmanned facilities, the sensor output shall trigger an audible alarm on site as well as in the facilities charged with alarm assessment and response force dispatch for that site. For these sites, the alarm shall not be deactivated at any time. At manned facilities the sensor output shall trigger an audible alarm on-site only. The alarm shall not be deactivated unless the perimeter fence gate is opened to accommodate heavy traffic (see paragraph 5.1.3.3.1.3).

5.1.3.3.6.1 Factors Influencing Choice of Sensors. No single sensor is available that detects all possible methods of intrusion into zone 1 and has an acceptable false alarm rate for the variety of site conditions found at DCS sites. Two or more sensors may be required to achieve a desired detection capability along with an acceptable false alarm rate. Each DCS site is unique in terms of the characteristics which influence the choice of exterior intrusions sensors. There is no single or combination of sensors that is applicable to all DCS sites. The choice of sensors shall be made after establishing the detection objectives of the zone 1 sensors and assessing all of the factors that can influence the decision (Table A-1). Assistance in the final choice and installation of zone 1 sensors shall be obtained from the U.S. Air Force Physical Security Systems Directorate, Hanscom Field, Bedford, Massachusetts.

5.1.3.3.6.2 Applicable Sensors. Based on the typical operating environment of manned and unmanned DCS sites, sensors applicable to zone 1 were rank ordered in terms of their applicability (Table A-2). Figures C-7 - C-10 present implementation details for the four highest ranked sensors. These details are presented solely to familiarize the user of this standard with the complexities of these devices.

5.1.3.3.7 Alarm Assessment and Procedures. An alarm triggered by a zone 1 sensor indicates the presence of one or more intruders inside the perimeter fence. The intruders' presence will be either authorized and, hence, predicted according to the site entry procedures specified in paragraph 5.1.3.3.2 or it will be unauthorized. For unmanned DCS facilities, assessment of the intrusion shall be made via two way audio

TABLE A-1

Site Characteristics to be Evaluated to Determine Appropriate Sensor Selection

Site Variations	- Soil conditions, pavement, ground freeze, streams, terrain, water lines, sewers, fence pole locations, buildings, underground cables
Environment	- Temperature, wind, rain, snow, wild life, thunder, lightning, earth vibrations, vegetation
Inherent Component Characteristics	- Sensor-to-sensor interactions, upkeep cost, stability, capability limitations, self-test, false alarm rate, probability of detection, cost, reliability, repeatability, tamper resistance
Man-Made Disturbances	- Underground telephone and power cables, generators, motors, power transformers, radio, T.V., radar, communications equipment, vehicle ignition, auto, train or aircraft vibrations
Human Engineering	- Ease of installation, ease of maintenance, assessment, reporting, personnel requirements
Interfaces	- Hardware/hardware, hardware/human, sensor/junction, sensor/data transmission links, sensor/power source available, sensor/installation hardware, sensor/tamper protection
Documentation	- Procurement, acceptance, installation, maintenance, software requirements, operational procedures, periodic checks, orderly checkout, test plans
Adversary Attributes	- Threat level, tools, weapons, methods of entry.

TABLE A-2. LIST OF SENSORS APPLICABLE TO ZONE ONE

	SENSOR/SENSOR TYPE	SOURCE
1.	Ported Coaxial Cable (PCC)	Military
2.	Individual Resource Protection Sensor (IRPS)	Military
3.	Magnetic Intrusion Line Sensor (MILES)	Military
4.	Bistatic Microwave	Commercial
5.	Point Sensor (Electromagnetic)	Military
6.	Electric Field Fence (EFF)	Commercial
7.	Laser Fence Sensor	Military
8.	Infrared Fence Sensor (IRCCD)	Military

equipment, the output of which is carried via voice grade channel to the site charged with alarm assessment and response force dispatch. Once a intrusion is verified, the response force shall be dispatched and a verbal challenge offered over the audio assessment system. At manned facilities, prompt visual assessment shall be made via CCTV. Once an intrusion is verified, the response force shall be dispatched.

5.1.3.3.8 Cables. All cables within zone 1 shall be buried according to the requirements specified in paragraph 5.1.3.2.5.

PORTED COAX CABLE SENSOR

Description - Ported Coax Cable is an exterior surveillance sensor designed to detect and locate intruders over long perimeters. It consists of an active electromagnetic sensor buried in the ground. The Ported Coax Cable Sensor is optimally employed at large sites with perimeters up to 3.2km in length.

Operation - Ported Coax consists of two identical "leaky" coaxial cables buried in the ground parallel to each other (Figure a). A pulsed transmitter is connected to one cable transducer and a receiver is connected to a second cable transducer. The operating frequency transmitted is in the 60 MHz band (VHF). Peak transmitted power is 800mw. The pulsed energy causes a surface wave to propagate along the outside of the transmit cable. A portion of this surface wave couples into the receiver cable producing a VHF return signal at the receiver. When an intruder enters into the electromagnetic field, this coupling between the transmit and receive cables is perturbed resulting in a change in the receive signal. Due to the nature of the short VHF pulse and the design of the ported cable, the location of the intruder is determined by the time delay between the start of the transmitted pulse and the reception of the profile disturbance. This system will simultaneously detect and locate multiple intruders.

Figure C-7. Ported Coax Cable Sensor

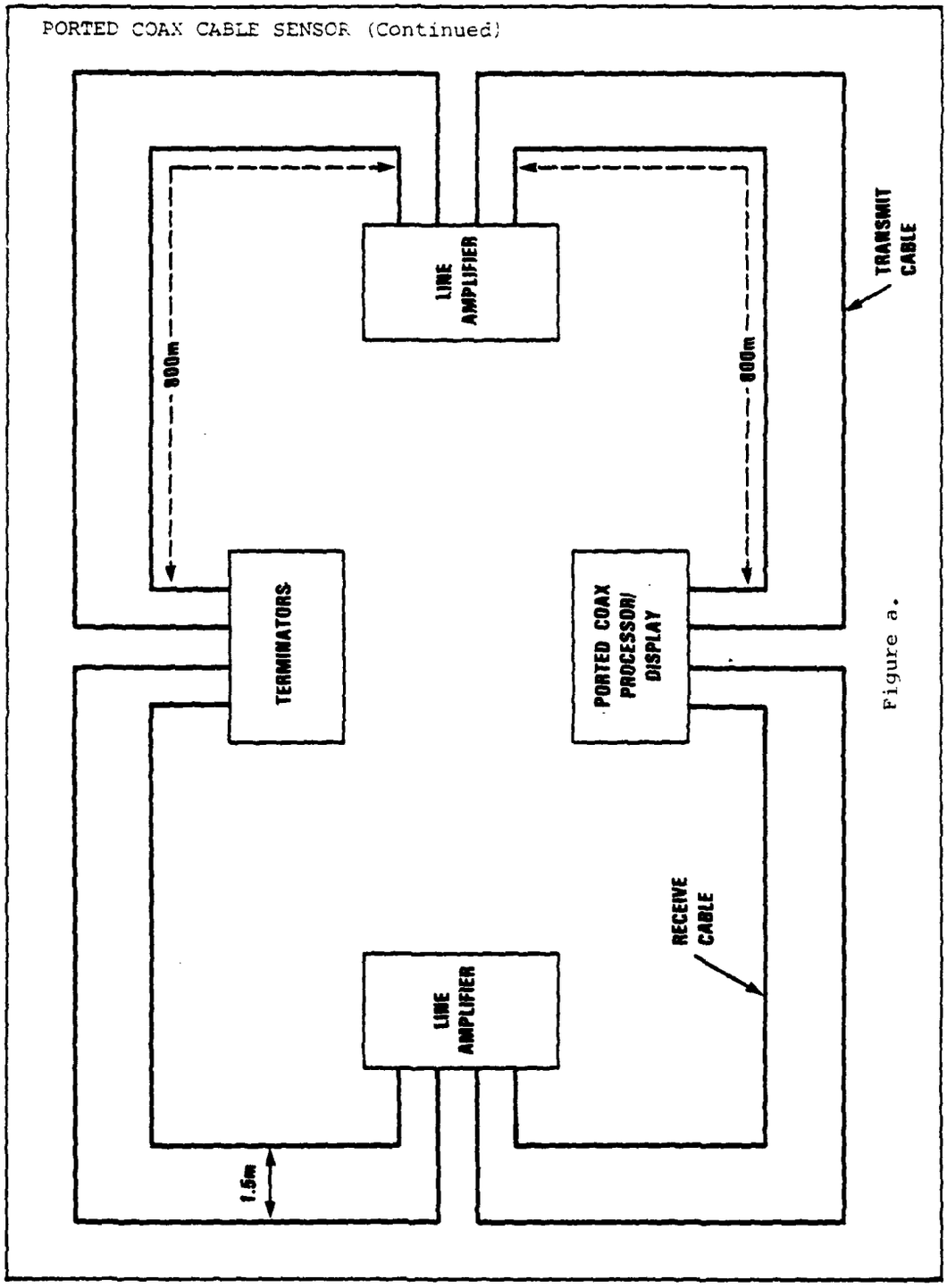


Figure C-7. (Continued)

PORTED COAX CABLE SENSOR (Continued)

Installation - A site compatibility test is recommended prior to procurement and installation because performance characteristics are not yet established. The site compatibility test consists of the installation of a short pair of ported cables. The transmit signal is applied while received signal power is monitored for both normal and water saturated soil conditions. The purpose of the test is to determine if the system is compatible with the soil conditions found at a given site.

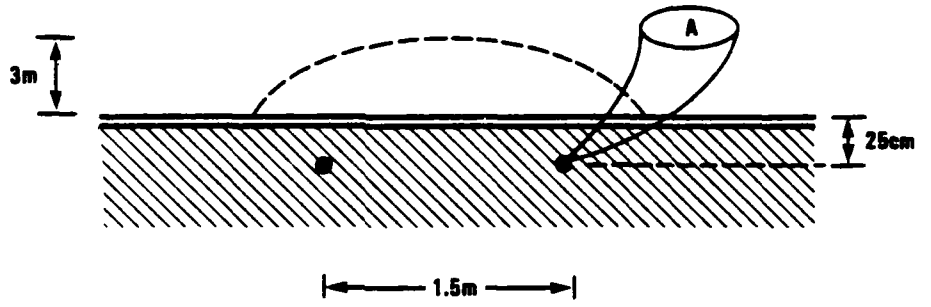
Upon actual system installation, the tolerance on both depth and cable separation is not critical. Recommended installation parameters are presented in Figure b. Uniform installation is recommended to enhance a uniform system response. The burial surface should be graded to promote water drainage. With a separation of 1.5 meters, the vertical coverage of the sensor is expected to be approximately 3m.

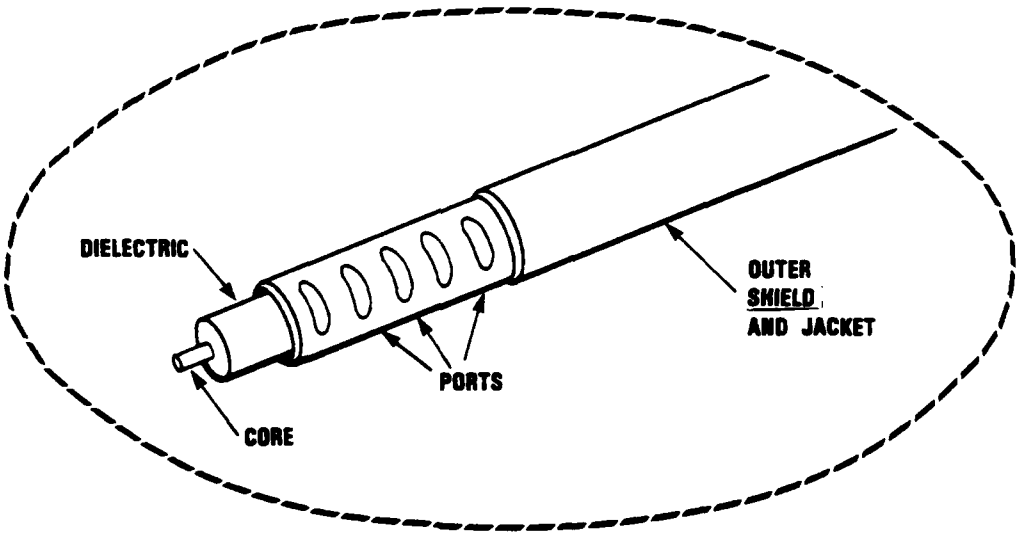
Maintenance - Department of Defense guidelines shall be followed. A daily walk-through procedure to test the detection for each 100m sector is recommended. The system contains a continuous self test feature, including manual diagnostics and external test connections.

References - Intrusion Detection Systems Handbook, Vol I and II, Sandia Laboratories, Albuquerque, NM, July 1980.

Figure C-7. (Continued)

PORTED COAX CABLE SENSOR (Continued)





"A"

Figure b.

Figure C-7. (Continued)

INDIVIDUAL RESOURCE PROTECTION SENSOR (IRPS)

Description - IRPS is a microprocessor based, buried line intrusion sensor for use in providing intrusion detection over short perimeter segments up to 300m in length.

Operation - IRPS consists of two identical "leaky" coaxial cables buried in the ground parallel to each other (Figure a). A transmitter is connected to one cable transducer and a receiver is connected to the second cable transducer. The transmitter cable is energized with a 60 MHz CW signal that causes a surface wave to propagate along the outside of the transmit cable. A portion of this surface wave couples into the receiver cable producing a continuous return signal at the receiver. When an intruder enters into this electromagnetic field, the coupling between the transmit and receive cables is disrupted and results in a change in the receive signal. The IRPS system offers detection only, with no indication of the exact location of the intrusion along the 300 meter length of this cable.

Installation - A site compatibility test is recommended prior to procurement and installation because performance characteristics are not yet established. The site compatibility test consists of the installation of a short pair of ported cables. The transmit signal is applied while received signal power is monitored for both normal and water saturated soil conditions. The purpose of the test is to determine if the system is compatible with the soil conditions found at each site.

Upon actual system installation, the tolerance on both depth and cable separation is not critical. A recommended burial depth is 25cm with a cable separation of approximately 1.5 meters. Uniform installation is recommended to enhance a uniform system response. The burial surface should be graded to promote water drainage.

Maintenance - Department of Defense guidelines shall be followed. A daily walk-through procedure to test the detection for each 100m sector is recommended. The system contains a continuous self-test feature, including manual diagnostics and external test connections.

References - Intrusion Detection Systems Handbook, Vols I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure C-8. Individual Resource Protection Sensor (IRPS)

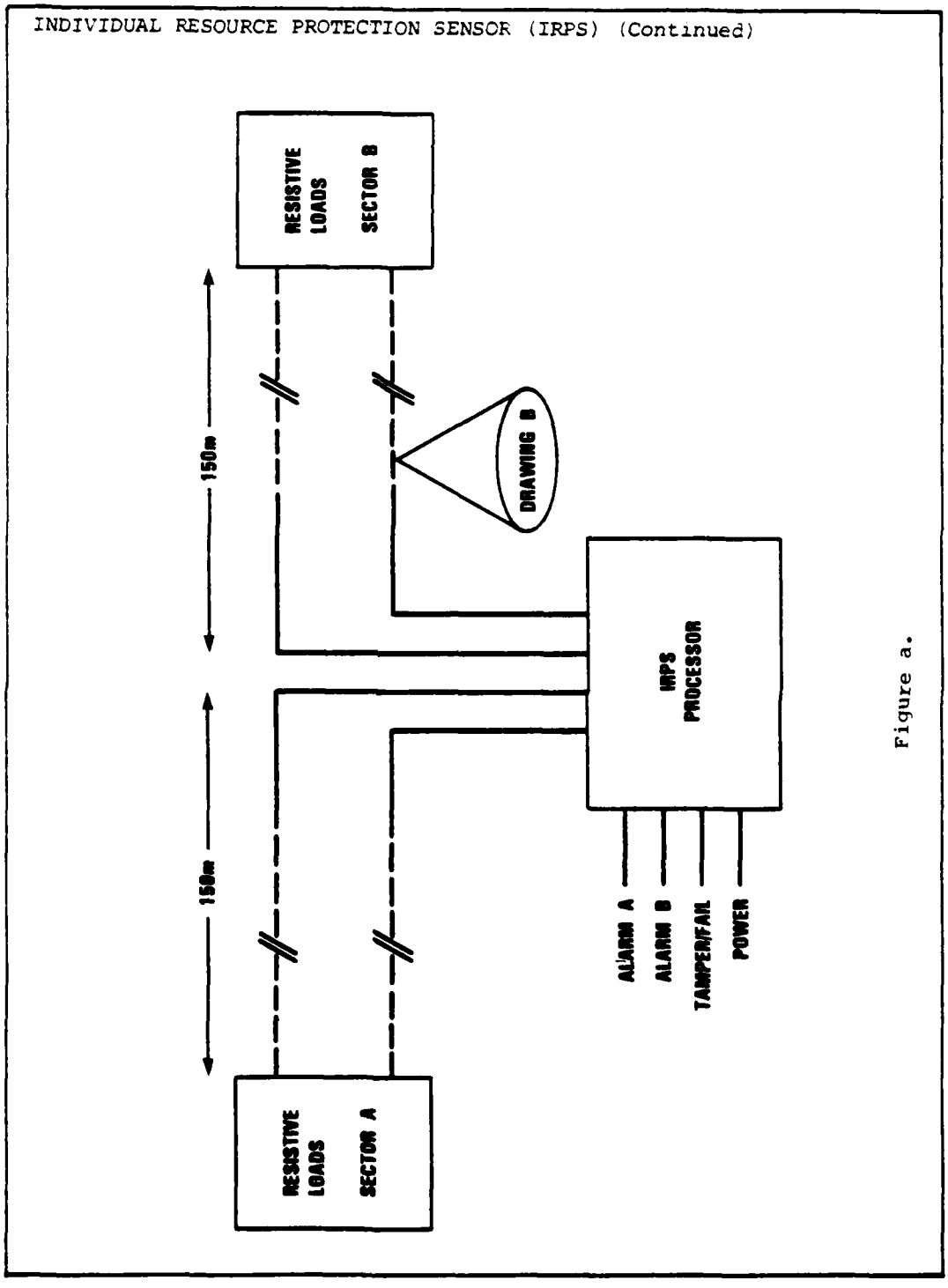


Figure C-8. (Continued)

INDIVIDUAL RESOURCE PROTECTION SENSOR (IRPS) (Continued)

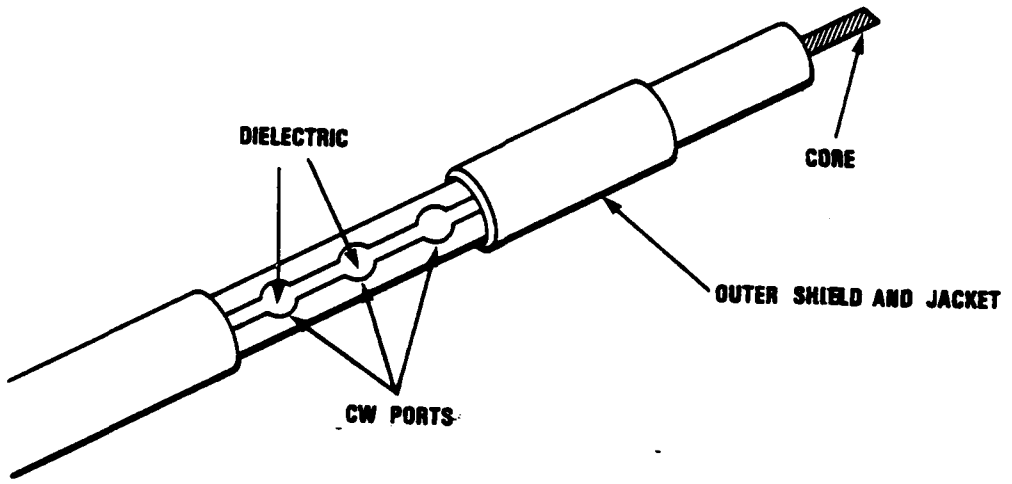


Figure b.

Figure C-8. (Continued)

MILES BURIED CABLE SENSOR

Description - The MILES, Magnetic Intrusion Line Sensor, buried cable is sensitive to both magnetic and seismic disturbances and is capable of sensing crawling, walking and running targets. The MILES sensor can detect intrusions independent of the presence of ferromagnetic material. MILES is the sensory cable for the MAID/MILES sensor. MAID is the electronic processor.

Operation - The MILES cable detection capability is based on the fact that motion disturbances will either move the cable in the earth's magnetic field or strain the cable's flexible magnetic core, thus changing the core's permeability (Figure a.) A disturbance will produce a signal in the sensing coil. If the response falls within a 4 Hz passband and exceeds a specified amplitude, an alarm is produced.

MILES is susceptible to false alarms from magnetic disturbances caused by lightning, power lines, buried power and signal cables and vehicle ignition noise. It is also susceptible to wind-induced ground motion and localized pressure sources such as moving vehicles, heavy equipment, and trains.

Installation - The MILES cable is installed in 100m segments. The sensor cable can follow irregular terrain. Mulitiple cables are overlapped as shown in Figure a. For each site installation of the MILES sensor, the depth of cable burial will differ. It is necessary to perform an initial test installation at each site to determine the optimum depth. To determine the best depth, one 100m cable is cut to make as many as nine 10m lengths. It has been observed that the background noise will increase approximately in proportion to the square root of the length of the cable and that the sensitivity is independent of the length. Using these facts, in conjunction with the initial test installation, the best cable burial depth at a given site is determined.

The cable is buried in accordance with Figure b. Installation is not recommended in asphalt or concrete unless the seismic capability of the transducer can be ignored. The following table provides some specific guidelines to be followed when installing the MILES transducer near potential seismic sources.

Figure C-9. Miles Buried Cable Sensor

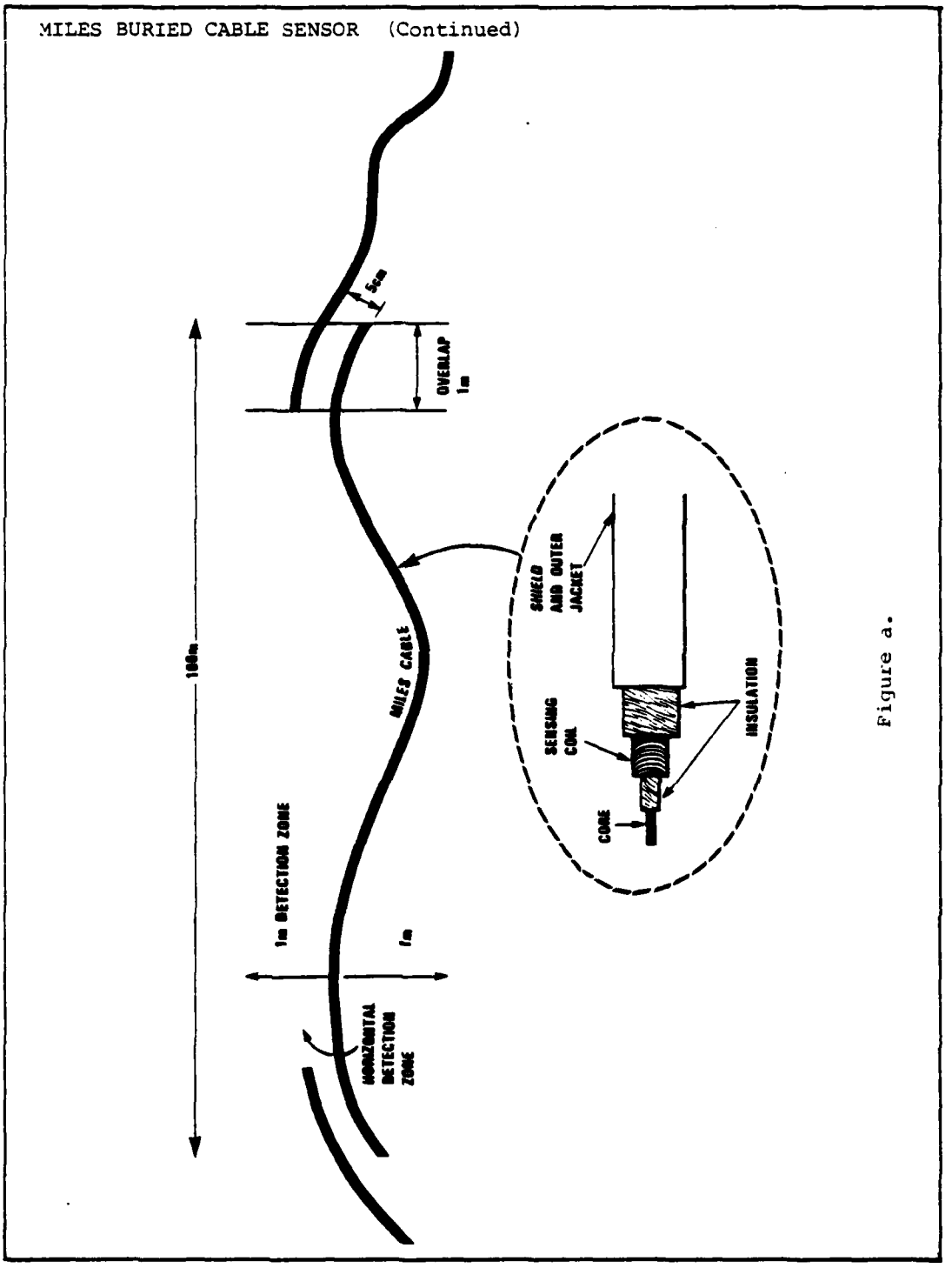


Figure C-9. (Continued)

MILES BURIED CABLE SENSOR (Continued)

Table of Guidelines

Source	Recommended Separation
Chain link fence	3m
Power poles	Equal to height of pole
Guy wires for power poles	6m
Tree drip lines	9m
Buildings housing machinery	6m
Roads with approx. 85 km/h traffic or heavy trucks	100m
Roads with approx. 16 km/h traffic and no heavy trucks	10m

Maintenance - The self-test feature of the MAID/MILES sensor shall be exercised at random intervals not to exceed one hour. Maintenance of the terrain, such as removing vegetation or filling eroded areas shall be performed as required. If the transducer is suspected of degraded performance, testing shall be initiated. Periodic performance testing is also recommended.

References - Intrusion Detection Systems Handbook, Vols. I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure C-9. (Continued)

BISTATIC MICROWAVE SENSORS

Description - Bistatic microwave sensors consist of an X-band source transmitting over a clear area of approximately 60 m to a receiver (Figure a). The transmitted signal is modulated at an audio frequency to form an amplitude sensitive beam breaking system. Multiple sensors are required to cover large perimeters and corners.

Operation - A bistatic microwave sensor is a line-of-sight device. The volume encompassed by the sensor is depicted in Figure b. The transmit antenna propagates a modulated signal toward the receive antenna. Terrain features, mounting height of the antennas, phase relationships and other characteristics determine the received signal strength and the offset which is the distance on the ground relative to the transmitter or receiver through which an intruder can crawl without detection. With an unauthorized entry into the detection zone, a portion of the transmitted energy will be deflected away from the receive antenna resulting in a change in signal strength and an alarm sequence will be initiated.

The microwave sensor is susceptible to the crawling intruder and to tampering. In addition, the area between the transmitter and receiver must be kept clear of all obstructions including grass or vegetation to maintain a suitable false alarm rate.

Installation - Prior to installation of a bistatic microwave sensor the coverage area shall be prepared in the following manner:

- Grass and weeds shall be controlled by soil sterilization or surfacing.
- Raised features shall be graded and depressions filled in order that no site discontinuities over 3 cm in size exist.
- The surface may be dirt, gravel, asphalt, concrete, or any combination as long as heavy rainfall will not cause errosion of the surface.

Figure C-10. Bistatic Microwave Sensors

BISTATIC MICROWAVE SENSORS (Continued)

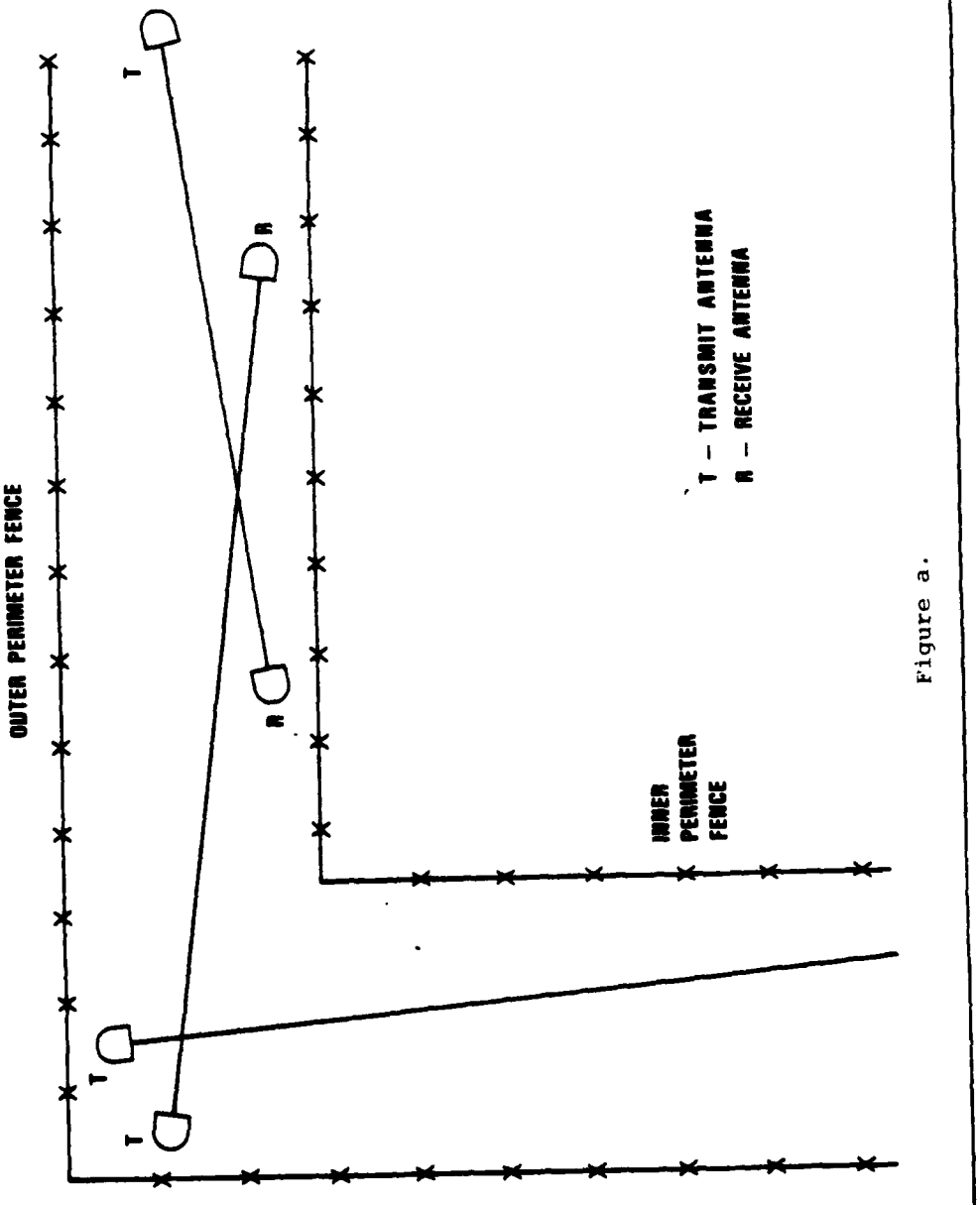


Figure a.

Figure C-10. (Continued)

BISTATIC MICROWAVE SENSORS (Continued)

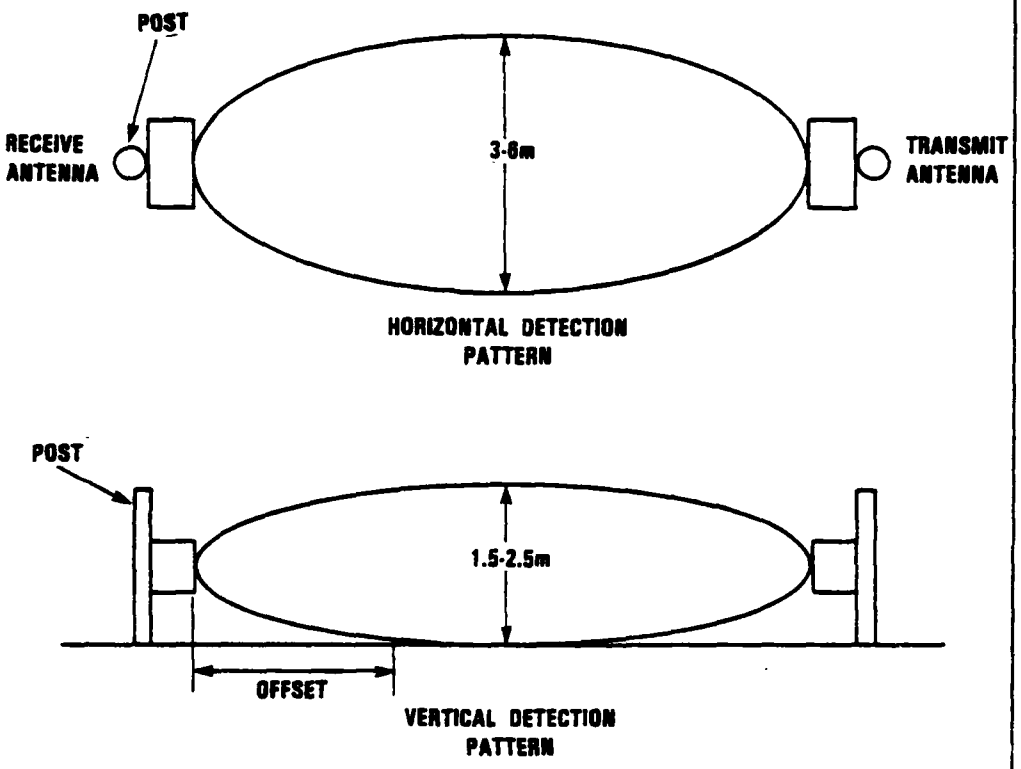


Figure b.

Figure C-10. (Continued)

BISTATIC MICROWAVE SENSORS (Continued)

- Structures such as towers, buildings, and fences shall be separated sufficiently from the microwave beam center line so as to not cause reflections which would degrade the system performance.

- If deep snow is a problem at the site, snow fencing shall be employed.

The installation of the sensor mounting post requires a fixed location steel pipe embedded in concrete. The system requirements, such as number of sensors to be mounted, will dictate pipe diameter and length. The pipe shall be installed as near to vertical as possible. All exposed signal lines shall be enclosed in conduit. All connecting signal wires shall be run underground in conduit.

Final elevation and azimuth alignment shall be carried out as recommended by the particular sensor manufacturer.

Maintenance - Periodic testing and maintenance is necessary to ensure system reliability and performance. A regular complete maintenance test shall be performed when the system is suspected of performance degradation or every 6 months.

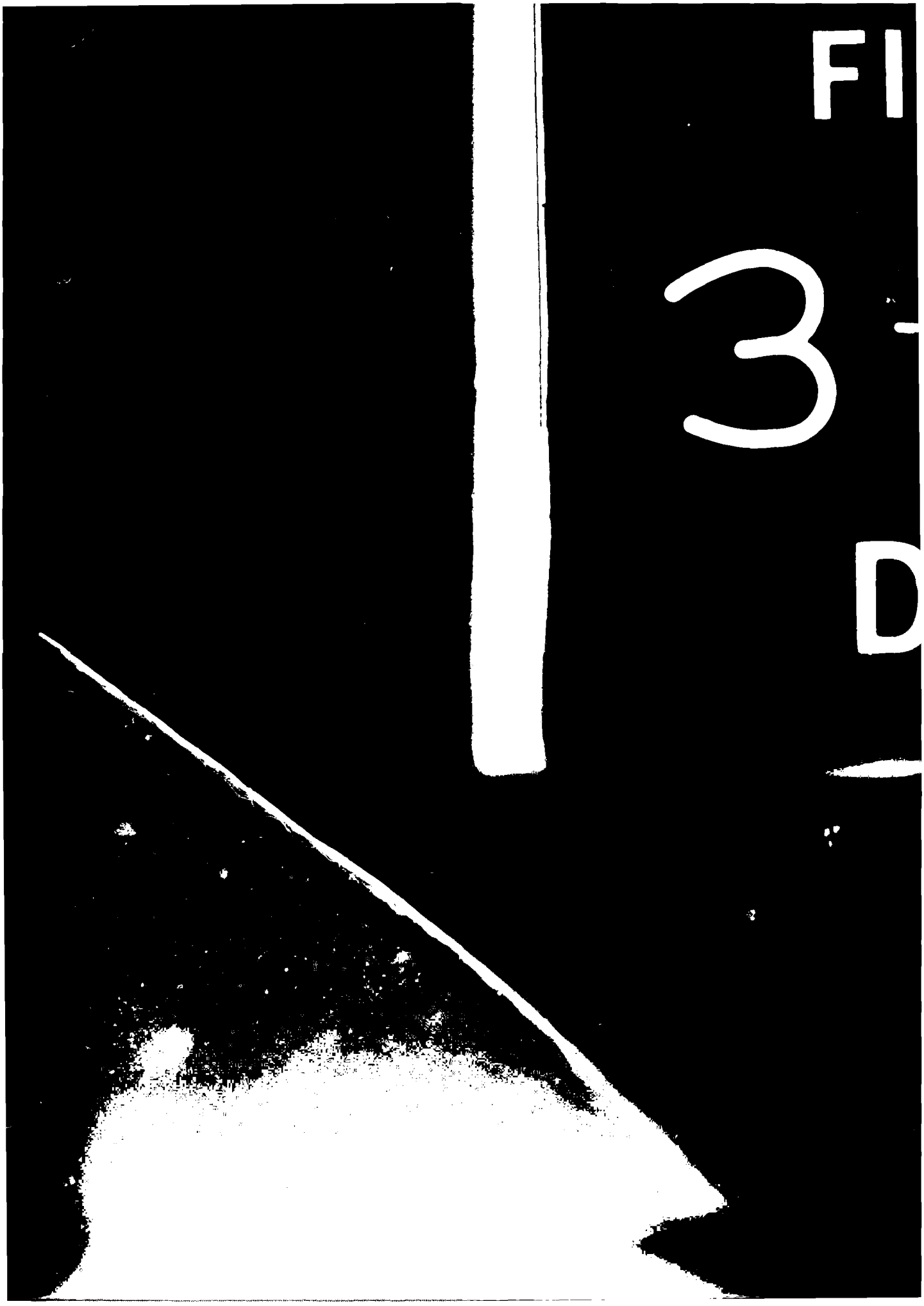
References - Intrusion Detection Systems Handbook, Vols. I and II, Sandia Laboratories, Albuquerque, New Mexico, July 1980.

Figure C-10. (Continued)

DISTRIBUTION LIST:

Administrator
Defense Technical Information Center
Attn: DTIC-DDA (12 copies)
(2 if classified or limited)
Cameron Station, Building 5
Alexandria, Va. 22314

Harry Diamond Laboratories
Attn: CO/TD/TSO/Division Directors
Attn: Record Copy, 81200
Attn: HDL Library, 81100 (3 copies)
Attn: HDL Library, 81100 (Woodbridge)
(Unclassified only)
Attn: Technical Reports Branch, 81300
Attn: Chairman, Editorial Committee
Attn: Legal Office, 97000
(Unclassified only)
(Add for reports from 21000/22000)
Attn: Chief, 20240


FI
3
D