



DEFENSE COMMUNICATIONS AGENCY  
WASHINGTON, D. C. 20305

DCA CIRCULAR 310-90-1

10 November 1983

**SURVIVABILITY**  
**Physical Security Measures**  
**for**  
**DCS Facilities**

1. Purpose. This Circular provides information and guidance to those activities responsible for implementing physical and procedural security measures. In addition, it facilitates the development of plans and programs to increase Defense Communications System (DCS) readiness, primarily through improvements in site security.

2. Applicability. This Circular applies to Headquarters, DCA, DCA field activities, and other governmental agencies responsible for the planning, programing, operation, or maintenance of components of the DCS.

3. References.

a. Defense Intelligence Agency Document DST-2610F-002-82, Threat to the Non-European Defense Communications System (U), SECRET/NOFORN/WNINTEL October 1982.

b. Defense Communications Agency Report, Defense Communications Under Stress (COMSTRESS) Phase II Report (U), SECRET/NOFORN/REL NATO, 12 March 1982.

c. MIL-HDBK-419, Grounding, Bonding, and Shielding for Electronic Equipments and Facilities, 21 January 1982.

d. Intelligence Agency Manual (DIAM) 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities, 2 May 1980.

e. Defense Communication System Facilities Survivability Enhancement (U), CONFIDENTIAL, 14 May 1982, U.S. Army Corps of Engineers, Huntsville Division.

f. DCA Circular 310-70-1, DCS Technical Control, Volume II, 22 September 1978.

g. DoD 5200.1-R, Information Security Program Regulation, August 1982.

---

OPR: B315

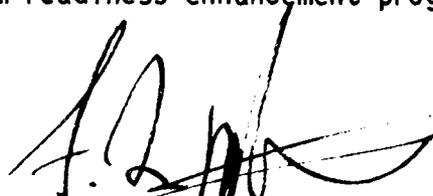
DISTRIBUTION: A, B, J through Q

4. General. The DCS is vital to the DoD and satisfies many critical communications requirements. To ensure appropriate DCS readiness, each element of the DCS must be analyzed and system vulnerabilities must be determined and corrected on the basis of a prioritization of sites, fixes, and fiscal resources available. Through the implementation of certain measures designed to eliminate or reduce identified deficiencies, the DCS can achieve improved readiness.

5. Procedures. This Circular is directed primarily toward implementation of short-term actions. However, when the nonavailability of financial or personnel resources prevents the implementation of these measures as short-term projects, the Planning, Programing, and Budgeting System (PPBS) process will be used. The guidance contained herein will enable users to:

- a. Identify site-related factors which decrease DCS readiness and survivability.
- b. Increase readiness and improve survivability.
- c. Provide a basis for the development of plans and programs to accomplish both near- and long-term readiness enhancement programs.

FOR THE DIRECTOR:



E. LEE MAYBAUM  
Colonel, USAF  
Chief of Staff

## CONTENTS

BASIC CIRCULAR	<u>Paragraph</u>	<u>Page</u>
Purpose . . . . .	1	i
Applicability . . . . .	2	i
References . . . . .	3	i
General . . . . .	4	ii
Procedures. . . . .	5	ii

<u>Chapter</u>	<u>Paragraph</u>	<u>Page</u>
<b>1. COMMUNICATIONS READINESS</b>		
Introduction. . . . .	1	1-1
General . . . . .	2	1-1
System and Facility Readiness . . . . .	3	1-1
Threats to the System . . . . .	4	1-1
<b>2. VULNERABILITY FACTORS</b>		
Introduction. . . . .	1	2-1
Operational Environments. . . . .	2	2-1
Site Considerations . . . . .	3	2-2
<b>3. PHYSICAL SECURITY MEASURES</b>		
Introduction. . . . .	1	3-1
Specific Measures . . . . .	2	3-1
Hardening of Site Components. . . . .	3	3-4
Physical Security Measure Costs . . . . .	4	3-8
<b>4. PROCEDURAL MEASURES</b>		
Introduction. . . . .	1	4-1
Security Procedures . . . . .	2	4-1
<b>5. READINESS PLANS AND PROGRAMS</b>		
Introduction. . . . .	1	5-1
Site Readiness Plans. . . . .	2	5-1
Exercises . . . . .	3	5-2
Operational Evaluations . . . . .	4	5-3
Summary . . . . .	5	5-3

<u>Chapter</u>	<u>Paragraph</u>	<u>Page</u>
<b>6. SAMPLE STANDARD OPERATING PROCEDURES FOR DCS FACILITIES</b>		
General . . . . .	1	6-1
Purpose . . . . .	2	6-1
Applicability . . . . .	3	6-1
Responsibilities . . . . .	4	6-1
Intelligence Threat . . . . .	5	6-2
Security Alerts . . . . .	6	6-2
Security Inspection . . . . .	7	6-2
Perimeter Security System . . . . .	8	6-2
Building Security . . . . .	9	6-4
Alarm Assessment . . . . .	10	6-4
Security Guard Force . . . . .	11	6-4
Personnel Protective Devices . . . . .	12	6-5
DCS Facility Readiness Checklist . . . . .	13	6-5

#### ILLUSTRATIONS

<u>Table</u>	<u>Page</u>
3-1 Approximate Unit Costs for Changes to DCS Installations to Enhance Survivability . . . . .	3-9
5-1 Summary of Vulnerability Factors and Security Measures . . . . .	5-4
6-1 DCA Facility Readiness Checklist . . . . .	6-6

## CHAPTER 1. COMMUNICATIONS READINESS

1. Introduction. The DCA ensures that the DCS is planned, improved, operated, maintained, and managed effectively, efficiently, and economically to meet the communications requirements of the National Command Authorities (NCA), the Office of the Joint Chiefs of Staff (OJCS), and the commanders of the unified and specified commands. DCS readiness must be consistent with this mission.

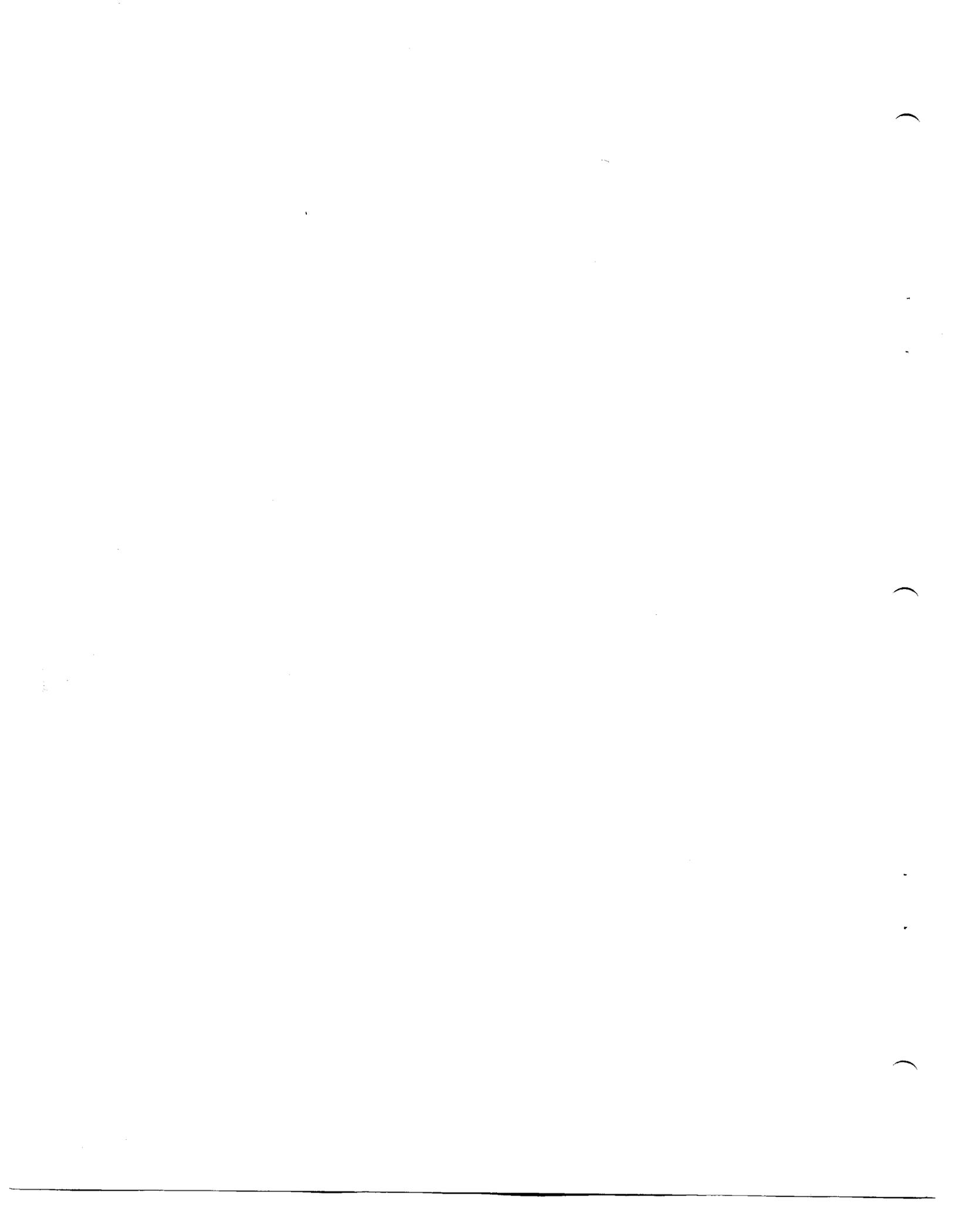
2. General. The security measures described in this Circular are primarily intended for Government-owned, -operated, and -maintained elements of the DCS, where local commanders can exert the greatest control. However, these measures also are desirable in other systems providing service to the DCS. While commercial carriers are not likely to readily implement physical modifications to their already constructed facilities, other existing features of commercial systems may be exploited to provide the protection required. Commercial capabilities in the United States can provide such readiness-enhancing features as redundancy and relatively rapid restoration. For commercial facilities overseas, foreign control or limited assets will affect the degree of protection provided, and greater reliance on U.S. Government-owned resources is necessary. Since they assume such critical importance, protection of U.S. Government-owned facilities in overseas areas should be given priority consideration.

3. System and Facility Readiness. Readiness of a communications system must be viewed from both a system and facility perspective as follows:

a. System Viewpoint. Readiness pertains to overall system capability and alternative ways to maintain that capability when segments of the system are lost. Ideally, the failure of a single site should not cause a catastrophic effect on the entire system or even on major portions of the system. However, the loss of several sites simultaneously could severely cripple the system.

b. Facility Viewpoint. Readiness also encompasses all physical and procedural measures which can be taken to decrease the vulnerability of the facility to catastrophic loss. For communications networks, system integrity depends on the simultaneous operation of interconnected sites. Countermeasures selectively applied at each site to increase resistance to local threats enhance the readiness of the entire system. Because the overseas DCS has limited flexibility in providing alternate transmission paths and switching facilities, the protection of individual sites in those parts of the world becomes vitally important.

4. Threats to the System. General threats to the DCS are addressed in references 3a and b. Both are available at DCA, Code B300. Threat information is available also from the various intelligence activities within the military services. The protective measures presented in this Circular are focused on increasing the level of protection of sites against vandalism and small arms fires and will provide some protection information on sabotage teams. The collateral effects associated with enemy air strikes on nearby targets will be discussed with regard to protection.



## CHAPTER 2. VULNERABILITY FACTORS

1. Introduction. Increasing DCS readiness requires the elimination or reduction of site and system deficiencies. In part, such shortcomings manifest themselves as vulnerabilities to manmade threats. Vulnerability, as used in this Circular, means physical weakness or susceptibility of a site, media, or personnel to an adverse external influence. The effects on DCS readiness can be physically or electromagnetically induced and generated by human or natural acts. This chapter briefly describes the vulnerability factors, in terms of operational environments, site considerations, and acts of nature.

2. Operational Environments. The DCS must be capable of performing its mission in situations ranging from peacetime to nuclear war. As hostilities increase, communications facilities may be subjected to a wide range of threats, including sabotage, direct physical attack, electronic warfare (EW), and chemical, biological, and radiological (CBR) warfare. The ability of the DCS to continue to provide service to remaining forces will depend on the degree to which security measures are effectively maintained. As the situation intensifies, readiness may deteriorate because the sophistication or multiplicity and diversity of force applied may become overwhelming.

a. Peacetime. The peacetime environment is characterized by the relative absence of international tension. The greatest physical threats to facilities during peacetime are those posed by dissidents or vandals, and by natural disasters, such as earthquakes and severe weather.

b. Transition to War. As international tensions increase, the threat to communications facilities increases accordingly. More incidents with dissidents can be expected, and sabotage becomes more likely.

c. Conventional Warfare. Conventional war, involving combat between opposing military forces using non-nuclear weapons, presents a wide range of threats to communications facilities. While major ground confrontations may be limited to relatively small geographical areas, the range and accuracy of air-delivered and ground-based missiles pose a real threat to any facility the enemy views as a worthwhile target, regardless of its location. References 3a and b present detailed information regarding the capabilities of Warsaw Pact countries and other potential adversaries.

(1) In conventional warfare, some communications facilities will likely be overrun and destroyed. Others will be neutralized by air or missile attack. Some will be targeted for attack by saboteurs. The resources applied by the enemy will depend on his perception of the importance of each facility from a command and control standpoint. The location of a facility far from the forward line of troops (FLOT) does not make it immune to attack.

(2) Hardening facilities to withstand the direct impact of today's conventional weapons, including standoff antitank weapons, is considered impractical. However, there are measures which can be applied to deter

saboteurs, increase resistance to small arms fires, and reduce the amount of damage caused by collateral weapons effects.

(3) Enemy use of chemical agents must be considered. The Soviet army, for example, has a formidable chemical warfare capability. The protection of a DCS facility against chemical attack entails both modifying the facility and a program to train personnel to operate in a chemical environment. Facility modifications may include collective protection systems such as filtration and positive pressure systems, as well as decontamination facilities.

d. Nuclear Warfare. Nuclear warfare lies at the extreme end of the conflict spectrum, and the limited use of nuclear weapons cannot be discounted. A nuclear-capable enemy may elect to expend nuclear weapons on selected targets. DCS facilities may be destroyed, damaged, or affected by other nuclear effects, such as electromagnetic pulse (EMP) and radiation, which are dependent upon many factors, such as distance of the facility from ground zero, weapon yield, and height of burst. This Circular does not address measures to counter the effects of EMP or radiation.

### 3. Site Considerations.

a. Proximity to the Battle Zone. Generally, the closer a communications facility is to the battle zone, the greater its susceptibility to attack or overrun. However, communications facilities in rear areas also are susceptible to direct and covert attack, especially if the enemy perceives them as vital C<sup>3</sup> nodal points.

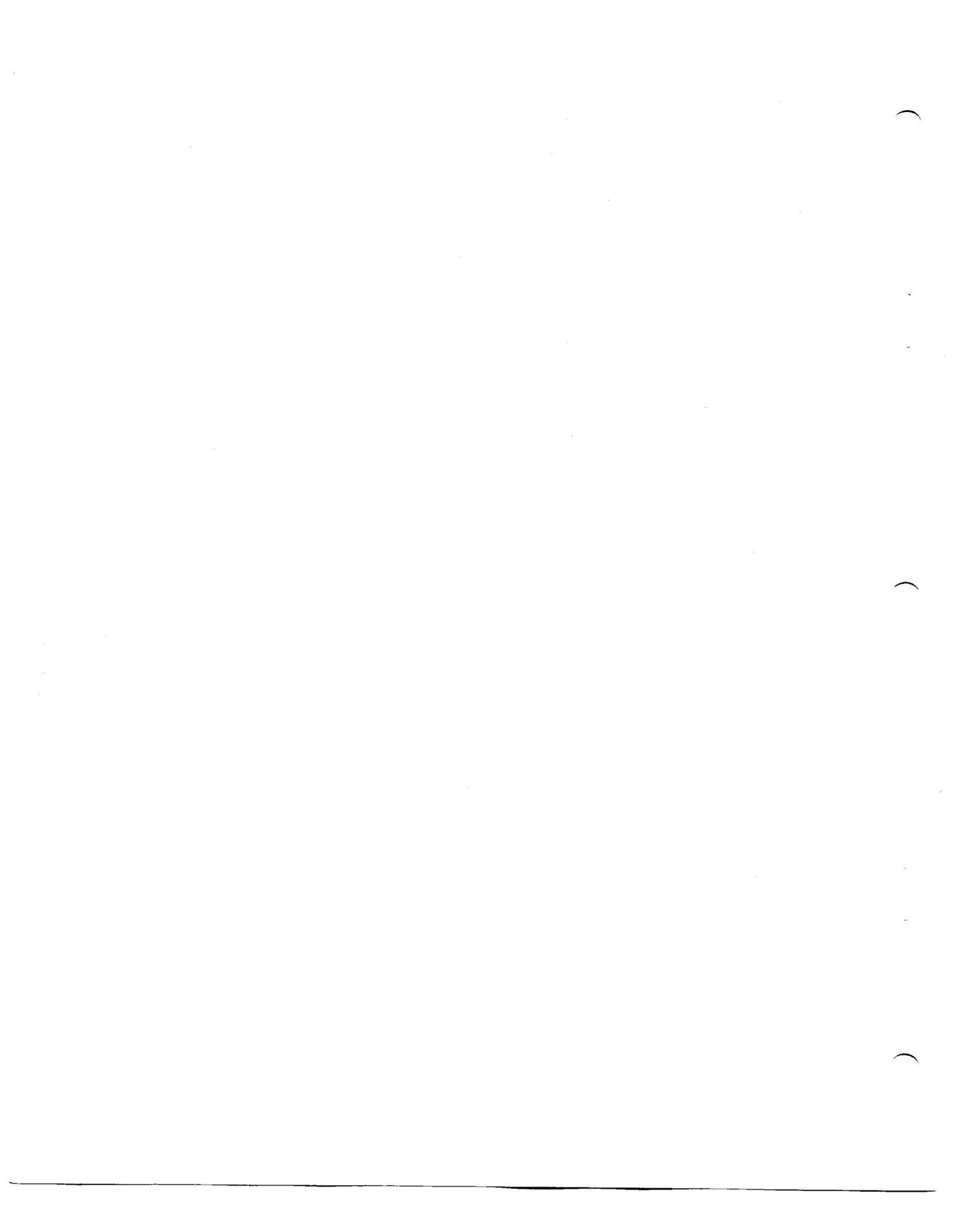
b. C2 Functional Importance. It should be assumed that the enemy is aware of the functions of DCS facilities in the theater command and control organization. This knowledge will be considered in his battle planning and his allocation and commitment of resources for neutralizing site capability. The greater the perceived importance, the more persistent will be the attack.

c. Exposure and Access. Site exposure and access are governed by the physical construction and topographical surroundings of a site. While some DCS facilities are located at prominent points on the landscape for operational reasons, others are tenant activities within larger military installations. Features, such as ease of access and the ability to clearly distinguish a communications function, will attract or discourage the use of a particular enemy capability. For example, an isolated and highly visible site may be a perfect candidate for neutralization by a diversionary force, whereas a tenant activity may be targeted by an air sortie.

d. Media Characteristics. The characteristics of a particular transmission medium will determine site configuration and, consequently, its vulnerability to certain external influences. Antenna size, signal type, and component equipment qualities are several factors which affect the method used and the ease or difficulty by which communications can be disrupted.

e. Facility Construction Characteristics. Existing DCS facilities were not designed for wartime use. As a result, many of the structures cannot withstand the blast effects of high explosives. The type of materials used in the construction of site buildings will significantly influence the overall vulnerability of the site.

f. Acts of Nature. Measures taken to reduce damage from the elements also provide some protection against the manmade threat. For example, where high winds are prevalent, extra precautions have been taken to guy antennas. Where snow loading on roofs is a problem, facility buildings have reinforced roofs. Generally, the more protection a facility has against the elements, the more capable it is of withstanding blast effects.



## CHAPTER 3. PHYSICAL SECURITY MEASURES

1. Introduction. Physical security measures are designed to reduce or eliminate deficiencies associated with such vulnerability factors as facility location, construction, layout, or housekeeping operations. They are directed toward improving the security of a site by altering its appearance, denying undetected intrusion inside the site perimeter, and contributing to the ability of the structures and other site components to resist damage by vandals or saboteurs.

2. Specific Measures. The following measures can be applied to enhance physical security at existing facilities.

a. Tonedown and Camouflage. Toning down buildings, towers, fuel tanks, and other site equipment is primarily intended to reduce visibility from the air. Tonedown can be accomplished by reducing or eliminating bright colors, reflective surfaces, or any other distinguishing features which set a communication element apart from the surrounding environment. Standard camouflage techniques can also be used; however, excessive use of camouflage may invite attention to the importance of a site. Insofar as possible, DCS sites should be made to resemble communications sites of the host nation.

b. Concealment Barriers. Although used primarily to harden facilities, manmade barriers can also be used for site concealment. Natural barriers such as hills, trees, or shrubs may also obscure a site from ground observation. On the other hand, such barriers may also make a site more vulnerable to ground attack, in that they may provide a degree of cover and concealment to the enemy. Use of barriers must be carefully considered.

c. Size Reduction. If technically feasible, reducing the size of a structure or communication component will normally reduce the ease by which it can be damaged or destroyed. For example, shortening the length of waveguide or reducing the diameter of an antenna reduces the exposed areas. Such measures may also include tower or dish replacement. Changes in component dimensions, however, must be weighed against the resultant impact on operational performance.

d. Access Roads. The number of roads leading to a communications site should be minimal and their use restricted, if possible, to personnel who have a requirement to be at the site. Critical communications sites or components (e.g., power substations) should not be located adjacent to public thoroughfares. Major facilities should have at least two access roads to circumvent isolation of the site due to natural phenomena or hostile action. Any actions taken to limit the use of access roads to a site must be thoroughly coordinated with host nation authorities.

e. Perimeter Fencing. When augmented with intrusion sensors, lights, and patrols, perimeter fences are positive means of enhancing site security.

(1) The site perimeter should be protected by a chain link security fence at least 7 feet high, topped with at least three strands of barbed wire. A double chain link fence, with the fences spaced 30 feet apart, is recommended. The topping should consist of a "Y" outrigger carrying the strands of barbed wire on each side, to which a roll of double-coiled barbed tape is fastened. The bottom of the fence should extend to within 2 inches of firm, level ground and be anchored to concrete curbs or sills so that intruders cannot easily go under the fence.

(2) The soil surface near the anchor should be compacted to prevent surface water from eroding loose soil and weakening the anchor. Drainage structures and water passages that penetrate the barrier and have a cross sectional area greater than 90 square inches should be protected by welded bar grills. As an alternative, drainage structures may be constructed of multiple pipes, each having a diameter of 10 inches or less.

(3) Fencing should be kept clear of all climbing vegetation.

f. Gates. A perimeter fence should have the minimum number of gates needed for vehicle and personnel access. Gates should be structurally similar to the fence and provide the same resistance to penetration. Gates should be designed so that traffic through them will be controlled. A guard should be posted at the gate to control access. If a gate guard is not used, the gate should be locked at all times. An intercom should be provided so that visitors can identify themselves. A cipher lock may be used for site personnel to gain access to the protected area. The gate should be observable and may be operated electronically from inside a nearby building. A buzzer should be activated when the gate is opened or unlocked.

g. Clear Zones. If not limited by site boundary restrictions or host country regulations, a clear area of at least 30 feet should be maintained on each side of the perimeter fence to prevent cover and concealment of an intruder. Clear zones for sites in nonforested areas should be free of all obstacles, vegetation, and topographical features exceeding 8 inches in height. For forested areas, only trees with limbs that extend over the perimeter should be removed. Other trees should have all branches lower than 10 feet above the ground surface removed.

h. Warning Signs.

(1) "NO TRESPASSING" signs should be provided to indicate that the area is restricted and that trespassers may encounter forceful ejection. Audible warnings may also be given by direct voice challenge or with sound-amplification equipment.

(2) Warning signs should be installed at intervals along the entire perimeter fence and at each entry point so they may be readily seen by anyone approaching the site. They should be placed so they do not aid intruder concealment or significantly obstruct the view from the site. In overseas areas the warning signs should be posted in both English and the local language. Signs should clearly state the dangers of trespassing in

restricted areas. Specific words used should be consistent with host nation requirements. The signs should not reveal the purpose of the site and be:

- (a) At least 1 foot high by 2 feet wide.
- (b) Painted with reflective material.
- (c) Legible at a distance of 50 feet.

i. Lighting. Perimeter lighting can be used as a deterrent to unauthorized entry and to facilitate the detection of intruders. Lights should be positioned within the site and along the entire perimeter. They should be configured and arranged to provide adequate illumination for personnel identification at the entry control point areas and in areas immediately surrounding the site, according to the following criteria:

(1) Perimeter lighting should be designed to enable the detection of persons throughout the region bounded by the inner perimeter fence (if double fencing is used) to 30 feet outside the outer perimeter fence. New lighting fixtures should be installed no closer than 8 feet inside the inner (or single) perimeter fence. At least 25 percent of the perimeter lighting should be protected from small arms fire.

(2) Perimeter lighting should not silhouette or highlight the security patrols, nor blind the sentries. The lighting should be under the control of the security force.

(3) The lighting system should produce full lumen output within 10 seconds after it is energized by either the prime power source or the emergency generator.

(4) The clear zones, which include the area between the fences when two are used, should be lighted to an intensity that will easily permit the security force to observe persons in those areas.

(5) The level of illumination at a distance of 30 feet beyond the outer fence should be adequate to enable visual detection of persons by security guards, or the operation of electro-optical (imaging system) or other electronic devices (if used) under various weather conditions.

(6) Perimeter lighting fixtures should be wired in parallel, so that failure of one or more lights does not affect the operation of the remaining lights.

j. Vehicle Parking. Private vehicles should be parked in a designated area outside the perimeter fence within view of the gate guard. Vehicles should not be authorized to park within 30 feet of a secure area or adjacent to critical components. Military vehicles should be secured inside the perimeter fence and should not impede the view of the perimeter.

k. Ladders and Fire Escapes. All special-purpose access ladders and fire escapes should be secured to prevent an intruder from gaining access to the roofs of critical buildings or to the antennas on microwave towers.

1. Intrusion Detection. An intrusion detection system may extend the limited capabilities of the security guard force to detect unauthorized entry into restricted areas. Sensors can be used to assist in detection of intrusion into the site (including entry gate), building entrances, and weapons and ammunition storage areas.

(1) The intrusion detection system should be operated on a dedicated power source, with emergency backup capable of ensuring uninterrupted operations.

(2) The sensor should activate an audible alarm at a location which is constantly manned to alert personnel to a change in status and to facilitate monitoring. Sensor outputs should terminate on a display panel, located at a guard post monitoring station or the operations control center, which should indicate:

(a) Intrusions.

(b) Failures of, or tampering with, the intrusion detection system.

(c) Alarmed zones into which entry has been allowed.

(d) Activated alarm zones.

(3) When the DCS site lies within a large military base that has its own centralized security guard force and security responsibilities for the DCS facility, the intrusion detection system should also be monitored at the base security operations center.

m. Fire and Smoke Alarms. Early detection of fire will enhance the probability of maintaining service in such an event. Fire and smoke alarms should be installed in all manned DCS structures. Further, in planning new facilities, fire and smoke detectors, as well as fire extinguishing systems, should be included in the design.

3. Hardening of Site Components. Physically hardening a facility is intended to make it less vulnerable to the effects of most conventional weapons. Appropriate architectural design and use of special construction material are measures which can be used for new facilities. For existing facilities, several short-term and less expensive measures can be accomplished, at the local level, to reduce vulnerabilities. Several of these measures also limit the exposure of, or access to, a site, as discussed previously. Techniques which are effective against conventional weapons will also help protect against severe weather conditions and other natural phenomena.

a. Building Construction. Buildings to be considered consist not only of those housing communications equipment and personnel, but also those housing critical support equipment such as emergency generators. Hardening existing structures can be expensive. However, the following are relatively inexpensive measures that can be taken to partially overcome design or construction deficiencies:

- (1) Bricking up unnecessary windows and doors.
- (2) Installing security bars.
- (3) Securing ventilator ducts and louvers, or relocating them above ground level.
- (4) Placing signal and power feeder cables underground. (Landlines to offsite users, including connections to commercial telephone systems, need protection comparable to that provided for the site components; the volume of wires and cables typical of van-mounted facilities makes them highly vulnerable.)
- (5) Keeping manhole covers, cable vaults, and junction boxes (for underground power and communications cables) located outside buildings, but near the site, securely locked and alarmed.
- (6) Rerouting cables, if necessary, so that not all of them are accessible through a single access point.
- (7) Providing redundant underground cables (by different routes) to critical offsite users.
- (8) Installing hardened or reinforced doors.
- (9) Installing dampers to seal building ventilation systems during chemical attack outside the building.
- (10) Keeping gates, doors, windows, fuel tanks, and other apertures locked except when actually in use. Use padlocks of a high security type, especially on doors leading to critical areas. Fire exits should be alarmed and configured for one-way, emergency use only.

b. Firefighting Capability. Fire should be expected to accompany various manmade and natural events, or may occur as a result of spontaneous combustion. Preventive and protective measures include debris control, maintaining good housekeeping habits, sprinkling systems, fire-breaks, adequate fire-fighting equipment, and storage of all flammables in separate locked containers.

c. Secondary Fences. Secondary fences may be installed around particularly sensitive site components, to further delay sabotage attempts against such items as fuel tanks, antenna towers, and operations areas. Such fences should be augmented with intrusion detection devices or other surveillance methods.

d. Power Sources.

(1) Commercial Power. Most commercial power sources can be easily cut off without entry into the site proper by merely cutting cables or destroying the power line system. Whenever possible, power lines inside

and outside the site should be buried and their location kept hidden from the general public. Junction boxes connecting above ground and underground power lines should be located to make them inaccessible to unauthorized personnel. Transformers that supply commercial power should not be left exposed, unprotected, or readily accessible.

(2) Site Generated Power. Generators used as a primary source, or for backup power, can be made inoperable by attacking the fuel system or the generator themselves. Security measures include:

(a) Installing locking caps on fuel filler pipes.

(b) Burying fuel tanks and fuel lines.

(c) Constructing protective revetments around exposed fuel tanks and generators.

e. Antenna Towers and Supports. Antenna towers and antenna supports are vulnerable because of their visibility and large size. Measures which will reduce vulnerability include:

(1) Using smaller size antennas and towers (consistent with reliable operation) to provide a smaller target.

(2) Enclosing tower supports with concrete sleeves.

(3) Enclosing guy-wire anchors.

(4) Installing a fence about 10 feet from the base of the antenna tower to impede unauthorized access. The fence should have a single, locked gate or connect directly to the radio building.

(5) Erecting an equipment building around the base of a self-supporting tower.

(6) Erecting a shelter around each guy-wire anchor point, and installing a pipe sleeve around each guy wire of a guyed tower.

f. Antenna Waveguides, Reflectors, and Horns.

(1) Waveguides. Waveguides are lucrative targets. Damage to them is easily accomplished by cutting, pinching, or piercing. They are particularly susceptible to damage from small arms fire. A single piece of damaged waveguide may be repaired in three to four hours providing repair parts are available; however, multiple areas of damage, adverse weather conditions, and damage at extreme heights on the tower are all factors that could greatly prolong the repair time of a waveguide system. Hardening measures include:

(a) Enclosing waveguides in steel ducts to shield them from small arms fire, crimping, or cutting. This protection should be provided from the exit point on the communications building throughout the route to the antenna horn.

(b) Relocating horizontal waveguide runs a minimum of 10 feet above the ground.

(2) Reflectors and Horns. Protective measures may be taken to prevent small arms fire damage to reflectors and horns by covering antennas with radomes, whenever operationally feasible, to limit feedhorn visibility and access. Installation of microwave antenna shrouds would also increase protection.

g. Revetments. Protective revetments add significantly to the hardening of a facility. Revetments can be made of brick, concrete (precast or cast in place), metal walls, sandbags, or mounds of soil. The material chosen will depend on the size of the area to be protected, available funds, available protective materials, and degree of threat. Some common types of revetments include:

(1) Sand-Filled Drum Revetments (6 feet high). Two offset rows of sand-filled 55-gallon drums stacked two high on an 8-inch concrete foundation. Adjacent drums are structurally joined by 1-inch steel rods and capped with 8 inches of concrete, allowing the revetment to function as a unit.

(2) Sand-Filled Culvert Pipe Revetments (6 feet high). Two offset rows of sand filled culvert pipe, 6 feet long and 2 feet in diameter, set vertically on an 8-inch concrete foundation. Adjacent pipes are structurally joined by 1-inch steel rods and capped with 8 inches of concrete, allowing the revetment to function as a unit.

h. Cooling Equipment. Two especially soft components at many facilities are the water cooling equipment required for some transmitters and the air-conditioners needed to keep other critical components operating. These types of equipment are easily damaged and are often exposed and vulnerable to attack. Consideration should be given to using revetments to protect them.

i. Air Intakes. Intakes should be protected against the introduction of flammable material and gases, especially where no flapper valve is provided.

j. Personnel Protection.

(1) The facility protection measures outlined above will help provide a degree of personnel protection. Other measures include availability of helmets, flak vests, gas masks, or other protective clothing. At overseas locations, this equipment should be stored onsite and maintained in condition for immediate use.

(2) Establishment of a fully equipped, self-contained shelter for offduty personnel should be considered. Such a facility should include a stock of essential supplies such as fuels, food, water, and emergency medical supplies.

4. Physical Security Measure Costs. Table 3-1 summarizes approximate costs for implementing various measures. The figures are based on research associated with a Corps of Engineers survey conducted at U.S. Army sites in Germany in 1982. The results of this research are presented in reference 3e.

TABLE 3-1. APPROXIMATE UNIT COSTS FOR CHANGES TO DCS INSTALLATIONS TO ENHANCE SURVIVABILITY<sup>1</sup>

Security Measures	Unit	Cost
<u>Intrusion Deterrence</u>		
Clearing and grubbing . . . . .	sq yd	\$ 1
Site grading. . . . .	sq yd	2
New perimeter fence . . . . .	lin ft	35
Fence repair. . . . .	lin ft	4
Vehicle barrier gate. . . . .	each	1,000
Perimeter lighting. . . . .	lin ft	2
Alarm . . . . .	each	600
Perimeter intrusion detection system with alarm . . . . .	each	6,400
Closed circuit television system. . . . .	each	5,000
Intrusion detection (door). . . . .	door	600
Intrusion detection (room). . . . .	room	800
<u>Blast Protection</u>		
Block window (1/4" steel or masonry). . . . .	sq ft	8
Armor 500-gallon day tank . . . . .	each	1,250
Bury fuel tank. . . . .	each	10,000
Shield air-conditioning condenser . . . . .	each	1,500
Shield substation (Masonry or 1/4" steel plate) . . . . .	job	1,500
Shield fuel pumps and line. . . . .	job	3,000
Shield diesel engine radiator . . . . .	each	1,000
Protect antenna tower base. . . . .	each	1,600
Armor waveguides and bridge . . . . .	lin ft	25
10' high masonry wall . . . . .	lin ft	60
10' high 1/4" steel plate for wall. . . . .	lin ft	100
Metal grid for ceiling. . . . .	sq ft	2.50
Cover for 30' antenna dish. . . . .	each	14,000
<u>Fire Protection</u>		
HALON fire protection . . . . .	sq ft	6.50
CO <sub>2</sub> fire protection . . . . .	sq ft	3.50
Sprinkler fire protection . . . . .	sq ft	3
Gypsum board ceiling. . . . .	sq ft	1

<sup>1</sup>Information presented in this table was provided by the U.S. Army Corps of Engineers, Huntsville Division, based on a survey of 12 Army-operated DCS sites in Germany in 1982.

TABLE 3-1. APPROXIMATE UNIT COSTS FOR CHANGES TO DCS  
INSTALLATIONS TO ENHANCE SURVIVABILITY (CON.)<sup>1</sup>

Security Measures	Unit	Cost
<u>CBR Protection</u>		
Eight CBR detectors with ancillary equipment. . . . .	job	\$ 8,000
Seal building penetrations for CBR. . . . .	each	4,000
CBR decontamination area. . . . .	each	20,000
CBR enclosure . . . . .	each	1,500
CBR entry air lock. . . . .	each	5,000
HVAC filter for CBR . . . . .	sq ft	6.25
New HVAC system . . . . .	each	25,000
Drinking water storage. . . . .	each	200
<u>Transient Current Protection</u>		
Separate fence from ring ground . . . . .	each	500
Shield and bond rooms, wall, floor, and ceiling . . . . .	sq ft	13
Shield door . . . . .	each	1,500
Power building, transient shielding and localized protection. . . . .	each	5,000
Entry power line filter . . . . .	each	500
Line filters and panels . . . . .	each	5,000
Entry and exit panel for waveguide and coax cable. . . . .	each	100

<sup>1</sup>See footnote on page 3-9.

## CHAPTER 4. PROCEDURAL MEASURES

1. Introduction. Procedural security measures are administrative or operational and are intended to contribute to the protection of sites from hostile acts. Certain procedural actions affect day-to-day operations; others are activated only as a situation develops. Procedural and physical security measures should be complementary and frequently reviewed, assessed, and updated.

2. Security Procedures. Procedural security measures should be directed toward the creation of a high readiness posture, characterized by personnel awareness and pride in being prepared for any eventuality.

a. Alerts and Training.

(1) Security alerts and training exercises should be conducted on a routine, unannounced basis to familiarize personnel with various security threats, to achieve a high degree of personnel readiness, and to enable personnel to quickly and efficiently master sound defensive practices. Advance warning should be given only when new equipment and procedures are being implemented or when new personnel are being trained.

(2) To the extent possible, site personnel should be trained to repel penetration and seizure efforts by saboteurs, terrorists, subversive elements, or other hostile forces. A security alert plan should be developed so that assigned personnel know their specific responsibilities. The plan should include alert procedures, emergency actions for various security contingencies, surveillance techniques for site protection, and procedures for control of site utilities and antisabotage devices.

b. Inspections. Site inspections should be conducted routinely and at irregular intervals by a survey team. The survey team should:

(1) Evaluate the defensive posture of the site and personnel readiness to curb sabotage and terrorism.

(2) Recommend changes in practices and procedures for enhancing readiness.

(3) Determine compliance with applicable security standards and guidelines and the effectiveness of existing security practices and procedures.

(4) Include an alert training exercise as part of the inspection.

c. Guard Force.

(1) Functions and Responsibilities. A guard force should be maintained at the most critical DCS facilities to provide overall security. The posting of guards at lower priority facilities should be considered on a case-by-case basis and may be tied to a specific state of readiness or defense condition (DEFCON). The guard force should be assigned normal, routine security functions and also have emergency responsibilities to:

(a) Maintain a strong defensive posture and a high degree of readiness to curb and repel sabotage and terrorist attacks.

(b) Control access of personnel and vehicles to the site and its restricted areas.

(c) Maintain surveillance of restricted areas.

(d) Assess intrusion alarms in a timely and reliable manner.

(e) Muster promptly and deploy effectively an armed reaction force to counter hostile intrusion.

(f) Staff guard posts and provide roving patrols.

(g) Maintain a site visitor entry log.

(h) Enforce site regulations on material transfer and storage, vehicle parking, etc.

(2) Training.

(a) The security guard force should receive specific training in the performance of the following functions:

1. Combat tactics, including differentiation between inadvertent trespass and forcible or surreptitious penetration of the site.

2. Personnel control, including identification, escort, and apprehension.

3. Crowd and riot control.

4. Enforcement of regulations on material transfer and vehicle parking.

5. Operation and use of intrusion detection and alarm monitoring systems.

6. Operation and use of security communications equipment.

7. Use and care of assigned weapons.

(b) In an emergency, the security force should protect the site mission and personnel and, if necessary, ensure the authorized destruction of classified material and equipment before they are compromised. Onsite personnel should be trained on use of small arms, chemical warfare protective equipment, and first-aid techniques.

(3) Guard Posts.

(a) Armed guards should be posted to control access to the site. Guard posts should allow an unobstructed view of the site perimeter and the operations center. They should be hardened against small arms fire and have a dedicated underground cable link with the operations center. The security guard should provide periodic status reports to the operations center.

(b) Duress alarms should be provided for the security force. One alarm should initiate a loud siren for the general alerting of all site personnel. A silent duress signal should also be provided to alert personnel without the intruder's being aware of the signal. A dedicated communications link should be provided between the operations center and the military police or local police stations.

(4) Patrols. An armed guard may be used to patrol the site perimeter in a random pattern. At periodic intervals (not to exceed 30 minutes), the guard should give status reports to the operations center by telephone or portable radio. Patrols may have to be intensified during hours of darkness or periods of reduced activity at the site.

(5) Backup Security Force. A backup security force of onsite personnel should be available to handle emergencies at all manned sites. Where a fulltime guard force does not exist, site personnel may have to provide the security services and, therefore, should receive basic security training. In small, isolated installations, all military personnel not primarily involved with physical security should be organized into a backup security force and assigned security duties in addition to their normal functions. The backup force should be under the direct command of the senior military member present, and be capable of immediate activation to provide:

(a) Short-term physical security assistance to the guard force.

(b) Emergency defense of critical buildings and vital areas, until additional defense units arrive from nearby military bases or local civil authority installations.

d. Access Control.

(1) Access to critical buildings or vital areas should be controlled through positive identification of all personnel as follows:

(a) A controlled picture badge system, preferably an exchange system so that the badges never leave the site. (This system would be practical only at facilities which have a large work force).

(b) A formal entry control roster.

(c) A visitor escort system and register.

(2) Entry into restricted or exclusion areas should be limited to authorized personnel (those needing to perform assigned tasks and including service, construction, emergency, fire, and medical personnel).

(a) Local nationals assigned to the site should be authorized entry to restricted areas only upon presentation of a valid pass; e.g., one issued by a designated military pass or registration authority.

(b) Local nationals not assigned to the site, but having official business within the facility, should be escorted by U.S. military personnel.

(c) Other U.S. forces personnel, maintenance personnel, contract personnel, and all others, to include local nationals desiring access to the facility, should obtain approval from the appropriate authority, who should notify the Site Chief of any intended visitors and their authorization to enter the facility.

(3) Upon arrival at the site, individuals should be required to present identification prior to entering the facility. Personnel requesting access to the site who have not obtained appropriate authorization should be denied access until the senior person on duty is able to confirm access authority.

e. Building Security. All buildings housing critical equipment or activities should be kept locked and alarmed when unattended, with access limited to a single door under the control of duty personnel. All other doors should be kept locked from the inside and alarmed.

f. Alarm Assessment. Intrusion alarms should be assessed by personnel at a central monitoring station and checked by direct visual observation of the alarmed zones. At some sites, because of the size of the installation and the configuration of the buildings and components, it may be necessary to dispatch a security guard. Electronic aids may also be used to preclude sending a guard to the alarmed zone. For example, such electronic devices as steerable or fixed closed-circuit TV cameras (normal, low light level, or infrared) may be advantageously installed on building roofs or radio towers to enable the direct observation of a zone that is otherwise obscured.

g. Weapons Control. The availability of weapons and ammunition to the security force is an important deterrent to intrusion. It establishes the installation as a defensible asset and increases personnel awareness that the site is a potential target of sabotage. Weapons and ammunition should be handled in accordance with appropriate DoD and military service regulations.

h. Community Relations. The relationship between communications site personnel and the local community is important to readiness, especially in foreign countries. The enmity of local nationals can be used against a site or its personnel. Community action programs involving local inhabitants will help improve understanding. A friendly environment will pay dividends in preventing tension.

i. Operational Procedures. Operational procedures for routing and re-routing circuits are outlined in reference 3f. The following factors should be considered in such planning.

(1) Area Avoidance. In certain geographic areas, communications

will be less secure than in others because of the local threat. Circuit routing through less vulnerable areas should be chosen to ensure a high degree of system integrity.

(2) Critical Nodes. Because of their importance, critical nodes must be considered lucrative targets and, therefore, more susceptible to attack. They should be avoided, if possible, when engineering service.

(3) Military Versus Commercial Facilities. The decision to use commercial facilities instead of military facilities can have a significant impact on readiness, depending on location. Infiltration of foreign commercial carrier facilities by unfriendly elements creates a potentially disruptive situation. Before a commercial lease is effected in an overseas area, this possibility must be considered. Other factors which may influence the use of commercial facilities instead of military resources are the availability of transmission media diversity and management policies of the individual military services.

(4) Restoration Priorities. Circuit restoration priorities must be considered when establishing communications service. Lower priority circuits should be placed on less secure paths and the higher priority circuits should be afforded greater protection through allocation and engineering measures.

(5) Alternate Routing. Alternate routing offers a means of increasing circuit availability. Contingency plans for alternate routing critical circuitry should be readily available and regularly exercised.



100  
100  
100



## CHAPTER 5. READINESS PLANS AND PROGRAMS

1. Introduction. Implementation of the security measures recommended in the preceding chapters will improve the readiness of the DCS. Toward this end, each DoD component capable of influencing the readiness posture of communication personnel and facilities must issue directives to stimulate appropriate action. The joint nature of the DCS requires that all DCS related plans and program prepared by the military departments and defense agencies be consistent in purpose so that the DCS assumes a uniform state of readiness. The general guidance which follows is intended to encourage the development of standard plans and programs.

2. Site Readiness Plans. Generalized procedural security measures are discussed in chapter 4. The following specific plans and programs may be used to implement such procedures; however, each plan or program must be tailored to fit the particular installation.

a. Site Defense Plan. Every site should have a Site Defense Plan covering all procedural aspects of security during various types of contingencies. It should include the following as a minimum:

(1) Procedures and Responsibilities. Detailed security procedures and responsibilities for all site personnel should be clearly outlined.

(2) Arms Control. Reaction to a crisis or a call for assistance normally will be rendered by onsite personnel. Weapons and ammunition must be stored on the premises and should be readily accessible for site defense. Access procedures and storage restrictions must not inhibit the use of weapons or ammunition, when authorized. Local regulations; e.g., the Status of Forces Agreements (SOFA); may limit or prohibit the use of weapons by U.S. personnel and should be reviewed. Such restrictions may seriously reduce the effectiveness of the site defense plan. These situations should be referred up the chain of command.

(3) Reaction Force. An offsite reaction force consisting of regular military forces, security police, local civilian police, or others, should be organized, wherever possible, to assist site personnel. Agreements should be made to assure the presence of such a force when requested, and procedures should be exercised to test effectiveness.

(4) Protection of Unmanned Facilities. The defense of unmanned facilities must also be considered. Intrusion detection and transportation of reaction forces are primary considerations. The use of helicopters to transport reaction forces may be appropriate.

(5) Destruction Plans. Emergency plans for sensitive equipment, key lists, and other national security information should be reviewed for compliance with the requirements of DoD 5200.1-R. Emergency plans for COMSEC destruction should be exercised quarterly.

b. Nuclear, Biological, and Chemical (NBC) Plan. Plans incorporating precautions and procedures to be followed during nuclear, biological, or chemical attack should be prepared and rehearsed.

c. Severe Weather Plan. A severe weather plan should be prepared. It should include, as a minimum, procedures for adequate warning and emergency operations.

d. Security Training Program and Plan. A security training plan should be prepared and a training program implemented to ensure that all personnel are familiar with site vulnerabilities and are prepared to react to crisis situations. Training curriculums should emphasize:

(1) Physical Security Threats and Associated Security Measures.

Every person assigned to a DCS facility should be thoroughly versed on the vulnerabilities and means available to resist physical threats. While each site will be different from all others in the details, the principles outlined in this Circular should form the basis for such training.

(2) Electromagnetic Threats and Associated Countermeasures.

Operator effectiveness is a function of knowledge, training, and equipment capability. Since much of the equipment used in the DCS is susceptible to electronic disturbances, the ability of the operator to recognize the cause of such disruption or interference at an early stage and to take actions necessary to maintain communications is essential to effective operations. A current and continuing training program for DCS communications personnel should be vigorously pursued to promote operator knowledge and to increase countermeasures proficiency. The program should include a balance of academic and practical training and be administered at the facility level.

(3) Personnel Conditioning. Besides training in security procedures and protection skills, the need to develop and maintain the mental and physical conditioning of site personnel should not be ignored. Defenders must be imbued with a positive attitude and encouraged to retain the physical stamina to resist a given threat. The availability of weapons will help instill confidence and reflect the seriousness of site defense. Personnel should also be kept advised whenever a lack of resources prevents the immediate accomplishment of readiness enhancement measures.

e. Physical Security Enhancement Program. Each level of command should develop and implement a Physical Security Enhancement Program for DCS facilities. It should include specific objectives and the means and procedures for achieving those objectives. It should be oriented toward self-help, low-cost (or no-cost) options that improve readiness. High-cost, long-term enhancements should be included in individual service programs and be reflected in the DCS Five Year Program (FYP).

3. Exercises. Exercises should be conducted periodically to ensure that personnel and equipment are able to overcome site vulnerabilities. The following areas should be included:

- a. Sabotage and security alerts.
- b. NBC alerts.

c. Reaction force drills.

d. Exercise of emergency destruction plans for sensitive material and equipment.

e. Alert and transportation drills for protection of unmanned sites.

4. Operational Evaluations. Operational visits by staff officers, Inspectors General (IG), and security experts can be used to evaluate the state of site readiness and can stimulate interest and actions. Formal inspections with reports should identify deficiencies and make specific recommendations for followup corrective actions.

5. Summary. Table 5-1 summarizes typical site vulnerabilities and the corresponding security measures which may be taken to reduce them. While it may appear that each measure listed has been categorized to pertain to a single vulnerability factor, it should be recognized that many of the recommended measures address more than one vulnerability.

TABLE 5-1. SUMMARY OF VULNERABILITY FACTORS AND SECURITY MEASURES

Factor	Prescription
<b><u>Site Exposure and Access</u></b>	
Site Visibility	Camouflage isolated sites. Use tone down painting to reduce visibility. Reduce size of site (if possible). Make site resemble those of host nation.
Perimeter Control	Prepare a clear zone 30 feet outside fence. Install adequate fencing, at least 7 feet high, with barbed wire topping. Anchor fence bottom and compact earth. Reduce number of gates to minimum. Structure same as fence. Lock gates when not in use. Install perimeter lighting to illuminate clear zone. Install bar grills over drainage openings. Install "restricted area" signs around perimeter both in English and in host nation languages. Install intrusion sensors. Install a secondary fence. Employ security guards and military working dogs.
Site Access Control	Control road access to site (if possible) Restrict vehicle parking to areas outside of and away from perimeter fence. Use a pass system to restrict access to those personnel whose duties require it.
<b><u>Blast Hardness</u></b>	
Building	Brick up unused entrances and windows. Install security bars on windows. Harden doors to same level as walls. Reinforce walls and ceilings. Secure ventilator ducts and louvers. Bury power and signal cable entrances into building.

TABLE 5-1. SUMMARY OF VULNERABILITY FACTORS AND SECURITY MEASURES (CON.)

Factor	Prescription
Antenna Towers and Waveguides	<p>Use smaller tower and antennas (if operationally feasible).  Encase tower legs and guy wires inside concrete or metal sleeves.  Install separate fence around tower base.  Enclose waveguides inside steel shrouds.  Install radomes over antennas (if operationally feasible).  Route waveguides for dispersion on tower.</p>
Other Critical Components	<p>Bury fuel tanks and lines.  Secure covers to cable access manholes.  Install revetments around air-conditioning units, emergency power units, aboveground fuel tanks, transformers, etc. Revetments may be made of brick, dirt and stone, concrete, sand-filled barrels, metal, and sandbags.</p>
<u>Nuclear, Biological, and Chemical (NBC)</u>	<p>Provide protective masks and clothing for all site personnel.  Maintain protected emergency stockpile of rations and water.  Install filtered air ventilation system.  Install NBC detection system.  Provide medical kits for emergency treatment of NBC casualties.  Conduct realistic training exercises.</p>
<u>Fire Prevention and Control</u>	<p>Burn off excess grasses around site.  Install smoke detectors and fire alarms in all manned areas and critical unmanned areas.  Maintain adequate firefighting equipment.  Conduct training, to include fire drills and exercises.</p>

TABLE 5-1. SUMMARY OF VULNERABILITY FACTORS AND SECURITY MEASURES (CON.)

Factor	Prescription
<u>Connectivity</u>	Use Mix of media; e.g., line of sight (LOS), leased, and satellite. For critical users, provide alternate paths, dual-homing, and redundancy. Stock adequate spares for repair of communications equipment failures. Route critical circuits to avoid high threat areas, including high density nodes.
<u>Readiness of Site Personnel</u>	Provide effective training program. Instill importance of mission in all personnel. Make weapons accessible for use. Train in site defense techniques. Conduct security alerts and exercises Provide for oncall, backup security force.

## CHAPTER 6. SAMPLE STANDARD OPERATING PROCEDURES FOR DCS FACILITIES

1. General. This chapter illustrates sample Standard Operating Procedures (SOP) as a guide to planners and DCS station personnel implementing security programs chartered by DoD and the military departments. An SOP should be developed and tailored for each DCS facility. General procedures and conditions at each site may vary considerably, and, in many cases, detailed procedures will have to be developed. Use of the terms Commander, DCS Detachment; Base Commander; Site Chief; and others is for illustration only. Actual titles will vary from site to site.

2. Purpose. The following SOP provides guidance on practices and procedures and site component configuration on design characteristics to increase the readiness of DCS facilities against acts of sabotage or other physical threats.

3. Applicability. The provisions of this sample SOP apply to all site personnel.

4. Responsibilities.

a. The Base Commander (or Site Chief) will:

(1) Ensure physical security of site facilities and will designate restricted or exclusion areas (any area where access is subject to special restrictions or controls for reasons of security or safeguarding of property or material).

(2) Establish priorities for protecting critical buildings and equipment.

b. The Physical Security Officer, under the Commander, will:

(1) Implement and supervise the overall physical security program.

(2) Make recommendations on upgrading equipment, devices, and procedures to delay intrusion and aid the security forces in detecting and apprehending intruders.

(3) Maintain a high degree of security awareness among site personnel.

c. Division and Section Chiefs will:

(1) Implement those physical security plans that apply to their respective areas and comply with the policies of the Base Commander.

(2) Report all potential and actual security violations to the Physical Security Officer.

d. Individuals will:

(1) Familiarize themselves with security regulations and procedures.

(2) Report potential and actual security violations to their division or section chiefs.

5. Intelligence Threat. The Base Commander will ensure that appropriate arrangements are made to receive intelligence reports and briefings by appropriate defense agencies, in a regular and timely manner, on extremist and subversive activities and incidents relating to sabotage, terrorist, or other threats to the site. All sources of useful intelligence, including those of host national and local law enforcement authorities, should be exploited. The Base Commander will take appropriate and timely actions commensurate with potential threat.

6. Security Alerts. In order to sensitize personnel to the "sabotage threat" and achieve a high degree of personnel readiness to curb sabotage, security alerts and training exercises will be conducted periodically on a routine, unannounced basis. Advance warning will be given only when new equipment and procedures are being implemented, or when new personnel are being trained. The training exercises will ensure that the security guards and all site personnel attain a high level of proficiency in quickly and efficiently establishing a sound defensive posture for protecting communications operations. Site personnel will be trained to repel penetration and seizure efforts by saboteurs, terrorists, and subversive elements.

7. Security Inspection. Site inspections will be made routinely and periodically to evaluate the defensive posture of the site, to evaluate personnel readiness to curb sabotage and terrorism, and to recommend changes in practices and by procedures for enhancing readiness. Compliance with applicable security standards and guidelines and the use of good security practices and procedures will be checked. A sabotage alert training exercise will be conducted as part of the inspection.

8. Perimeter Security System. A perimeter security system will be established to control access to the site and inhibit unauthorized entry. The perimeter security system should consist of an integrated system of fences, gates, clear zones, intrusion warnings signs, lighting and sensors, parking zones, and access control.

a. Access Control.

(1) Access to limited or exclusion areas will be controlled through positive identification of all personnel. One or more of the following controls should be used:

(a) A controlled picture badge system.

(b) A formal entry control roster.

(c) A visitor escort system and register.

(2) Entry into limited or exclusion areas will be restricted to authorized personnel. Personnel authorized access will be limited to those needing to perform assigned tasks, including service, construction, and emergency personnel (fire, medical).

(3) Local nationals assigned to the site will be authorized entry upon presentation of a valid gate pass (i.e., one issued and stamped by the site Security Officer). Local nationals having official business within the facility will be authorized entry and escorted by U.S. military personnel. Other U.S. forces personnel, maintenance personnel, contract personnel, and all others, to include local nationals, desiring access to the facility will obtain approval from the DCS Detachment Commander, who will notify the Site Chief of any intended visitors and their authorization to enter the facility. Upon arrival at the site, individuals will be required to present identification prior to entering the facility. Personnel requesting access to the site who have not obtained approval from the Commander, DCS Detachment, will be denied access until the Site Chief or senior man on duty is able to confirm access authority with the Commander, DCS Detachment.

b. Guard Post. At periodic intervals not to exceed 30 minutes, the security guard will give status reports to the operations center. The telephone cable between the gatehouse and operations center will be routed underground to its terminal points. A duress alarm will be provided for the security guard at the gatehouse. Activation of the alarm will initiate a loud siren for the general alerting of all site personnel. A dedicated communications link such as a base station radio will be provided between the operations center and the military police or local police stations.

c. Patrols. An armed security guard will routinely patrol the site perimeter in a random pattern. At periodic intervals, not to exceed 30 minutes, the security guard will give status reports to the operations center by a portable radio. Patrols will be intensified during the hours of darkness or reduced activity at the site.

d. Backup Security Force. A backup security force of onsite personnel will be organized or made available to handle emergencies at all sites. In small, isolated installations all military personnel not primarily involved with physical security will be organized into a backup security force and will be assigned security duties in addition to their normal tasks. The backup force will be under the direct command of the Commanding Officer and will be activated quickly to provide:

(1) Short-term physical security assistance to the guard force.

(2) Emergency defense of critical buildings and vital areas until additional defense units arrive from nearby military bases or local civil authorities.

9. Building Security. All buildings will be kept locked and alarmed when unattended. Buildings housing critical equipment or activities will be accessed through a single door under the control of duty personnel. All other doors will be kept locked from the inside and alarmed.

10. Alarm Assessment. Intrusion alarms will be assessed by the security guard at the monitoring station through direct visual observation of the alarmed zones. (At some sites, because of the size of the installation and the configuration of the buildings and components, security guards should be alerted to make a direct visual observation, or electronic aids may be provided to preclude sending a guard to the alarmed zone. For example, such electronic devices as steerable or fixed closed-circuit TV cameras (normal, low light level, or infrared) may be advantageously installed on building roofs or radio towers to enable the direct observation of a perimeter zone that is otherwise obscured).

11. Security Guard Force.

a. Responsibilities. A security guard force will be maintained at the site to provide overall security. It will be assigned normal, routine security functions and also will have emergency responsibilities. The function and responsibilities include, but are not limited to, the following:

- (1) Maintaining a strong defensive posture and a high degree of readiness to curb and repel sabotage and terrorist attacks.
- (2) Controlling access of personnel and vehicles to the site and its restricted and exclusion areas.
- (3) Maintaining surveillance of restricted areas.
- (4) Assessing intrusion alarms in a timely and reliable manner if a perimeter electronic intrusion detection system is used.
- (5) Mustering promptly and deploying effectively an armed reaction force to counter a threat of hostile intrusion.
- (6) Manning guard posts (guardhouses) and providing roving patrols.
- (7) Maintaining a visitor entry log and providing visitor escorts.
- (8) Enforcing site regulations on material transfer and storage, vehicle parking, etc.

b. Training.

(1) The security guard force will be trained and certified for proficiency in the performance of the following functions.

- (a) Personnel control, including their identification, escort, and apprehension.

(b) Enforcement of regulations on material transfer and vehicle parking.

(c) Operation and use of intrusion detection and alarm monitoring systems.

(d) Operation and use of security communications equipment.

(e) Use and care of assigned weapons.

(f) Specific combat tactics in order to differentiate between inadvertent trespassing and forcible, surreptitious penetrations of the site.

(2) The use of extreme force will not be allowed except as follows:

(a) When a forcible attempt is made to breach a specified safeguard or boundary, and there is a willful intent to damage or destroy the site.

(b) To protect the site mission and personnel and, if necessary, ensure the authorized destruction of classified material and equipment before it is compromised.

12. Personnel Protective Devices. Gas masks and protective clothing will be issued to all individuals and kept near their work stations. These devices will be inspected periodically to ensure operational effectiveness. All personnel will be scheduled for periodic training in the proper wear and use of gas masks and protective clothing.

13. DCS Facility Readiness Checklist. A comprehensive list of items critical to DCS readiness is provided in table 6-1. The checklist may be used as a guide from which appropriate directives can be formulated and implemented. A "yes" answer to each item indicates satisfactory and a "no" answer indicates that corrective action may be required.

TABLE 6-1. DCA FACILITY READINESS CHECKLIST

Item No.	Item To Be Checked	Yes No
1.	Is the sabotage and terrorist threat to the site periodically reassessed?	
2.	Have contingency plans been established for increased defense readiness under various threat conditions?	
3.	Are security needs adequately budgeted for?	
4.	Has a security alert team been established?	
5.	Has a backup reaction force been established?	
6.	Are the alert and backup forces properly equipped and armed?	
7.	Have site security procedures and plans been developed?	
8.	Have provisions been made for secure intrasite security communications?	
9.	Have procedures and facilities been established for emergency destruction of classified material and equipment?	
10.	Has liaison been established with nearby military bases and local authorities, including their intelligence and counter-intelligence units?	
11.	Have procedures been established for routine and emergency issue of weapons and ammunition?	
12.	Has storage of a limited supply of arms and ammunition been prescribed for immediate access in case of a surprise attack?	
13.	Are gas masks and protective clothing easily accessible by all site personnel?	
14.	Are site personnel trained in site defense tactics?	
15.	Are site personnel qualified to use their individual weapons?	
16.	Is the site perimeter fence in good repair?	
17.	Is the perimeter fence topped with an outrigger and barbed wire?	

TABLE 6-1. DCS FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
18.	Do clear zones exist on each side of the perimeter fence? (30 feet is recommended)	
19.	Are culverts, tunnels, manholes, cable vaults, and utility accesses secured?	
20.	Are gates secured and is access through them controlled?	
21.	Are warning signs posted and maintained to identify restricted areas?	
22.	Is perimeter lighting turned on automatically during hours of darkness or poor visibility?	
23.	Is adequate lighting provided for guard use and sensor application?	
24.	Are control switches, light poles, and guy wires located inside the perimeter, under the control of the security force?	
25.	Is the lighting system on an uninterrupted power source?	
26.	Is an escort provided for visitors and uncleared personnel?	
27.	Is a personnel identification system used for the control of site personnel, visitors, and uncleared personnel?	
28.	Is loitering near restricted areas or critical components prohibited?	
29.	Is a visitors log maintained?	
30.	Are building doors and windows secured and alarmed when the building is unattended?	
31.	Are oncall reaction forces trained in site defense tactics?	
32.	Are security alert training exercises and drills conducted by guards and reaction forces?	
33.	Is a duress alarm system installed and is its purpose and use understood by all site personnel?	

TABLE 6-1. DCS FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
34.	Have key buildings and vital areas been identified for defense by the security forces during emergencies?	
35.	Are signal and power cables routed through underground metal or concrete conduits and terminated in tamperproof cable vaults?	
36.	Do underground signal and power cables follow unmarked routes?	
37.	Are manhole covers and cable access vaults locked?	
38.	Are waveguide runs protected from small areas fire?	
39.	Are circuit breakers close to the equipment served?	
40.	Are substation transformers enclosed by an approved, locked fence?	
41.	Do emergency power generators start automatically when needed?	
42.	Are fuel tanks buried or enclosed within retaining walls?	
43.	Are filler caps, drain valves, and vent pipes for fuel tanks locked and tamperproof?	
44.	Are all fuel lines routed underground?	
45.	Are towers painted to resemble those of the host country?	
46.	Is the tower base enclosed by an approved locked fence?	
47.	Are antennas and feed horns covered with radomes?	
48.	Are air-conditioning units located in protected areas?	
49.	Are flammables, tools, and ladders locked up?	
50.	Are satellite antenna radomes accessible at ground level, secured, and sensed?	
51.	Does the security force have its own communications system?	
52.	Do guard patrols have radio communications with the operations center?	

TABLE 6-1. DCA FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
53.	Does the operations center have reliable communications with oncall reaction forces?	
54.	Is a perimeter intrusion detection system (IDS) installed?	
55.	Is remote monitoring provided for the IDS?	
56.	Does the IDS meet site requirements?	
57.	Are the IDS components and cables protected against physical damage or compromise?	
58.	Is the IDS fail-safe, and does it operate on an uninterrupted power source?	
59.	Are records and logs maintained on file to permit evaluation of the IDS effectiveness?	
60.	Are daily tests conducted to ensure that the IDS system is operational?	
61.	Is one set of transmission lines between the sensor or detection components and the monitor or annunciator panel completely contained within the secured area?	
62.	Are alarms acknowledged and assessed promptly?	
63.	Is a guard tower or closed-circuit TV platform used (when site location, terrain, and configuration are suitable) to observe the site perimeter and critical components?	
64.	Are individuals aware of their responsibilities in the use of "extreme force"?	
65.	Are individuals aware of their responsibilities regarding accountability of weapons, ammunition, and explosives?	
66.	Has a Physical Security Enhancement Program been established to develop plans for physical security enhancement projects?	
67.	Does the site Physical Security Enhancement Plan address the threats found in peacetime, periods of increased tension, and armed conflict?	

TABLE 6-1. DCS FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
68.	Is the Physical Security Enhancement Plan realistic?	
69.	Has a Site Defense Plan been prepared?	
70.	Is the Site Defense Plan reviewed periodically to ensure realism and comprehensiveness?	
71.	Is the Site Defense Plan exercised periodically?	
72.	Does the Site Defense Plan include: <ul style="list-style-type: none"> <li>a. Detailed procedures and responsibilities for all site personnel, including guard forces?</li> <li>b. Arms control?</li> <li>c. Reaction forces?</li> <li>d. Protection of unmanned facilities?</li> <li>e. Destruction plans?</li> </ul>	
73.	Are exercises conducted periodically to ensure personnel have the training and material necessary to react to an armed threat? Types of exercises should include: <ul style="list-style-type: none"> <li>a. Security alert and sabotage alert exercises.</li> <li>b. NBC alerts.</li> <li>c. Reaction force response.</li> <li>d. Destruction of sensitive items.</li> <li>e. Protection of unmanned sites.</li> </ul>	
74.	Have actions been taken to increase facility physical hardness?	
75.	In high risk areas, have unnecessary windows and doors been bricked up to prevent flying debris, etc., from damaging equipments?	
76.	Is facility upkeep adequate to prevent the accumulation of combustible materials?	

TABLE 6-1. DCS FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
77.	Is accessibility to backup power and supporting fuel systems controlled?	
78.	Are tower supporting structures hardened (if feasible and practical)?	
79.	Are sandbags or other protective revetments used to protect sensitive, exposed components?	
80.	Is personnel protection adequate?	
81.	Do alternate routing plans exist for a communications facility? Are they adequate?	
82.	Do plans exist to protect against nuclear, biological, and chemical (NBC) warfare?	
83.	Has a training program been developed to acquaint new personnel with site vulnerabilities, security measures, and procedures?	
84.	Are communications vulnerabilities and security measures an item of interest during staff assistance visits, inspections, or performance evaluations?	
85.	Are system operators aware of the procedures available to them to counter electromagnetic effects?	
86.	Are written instructions available to operators on how to use built-in equipment capabilities?	
87.	Has a Severe Weather Plan been developed which outlines actions that must be accomplished to minimize effects of severe weather?	
88.	At station level, are efforts made to ensure the facility electrical and signal grounding systems are operating properly and that their integrity is maintained.	
89.	At those facilities where installed, are electromagnetic protective devices maintained and checked periodically to ensure their integrity?	
90.	Are protective barriers constructed (in high risk-areas) that will limit an enemy's access to a site and which will also help to harden the facility?	

TABLE 6-1. DCA FACILITY READINESS CHECKLIST (CON.)

Item No.	Item To Be Checked	Yes No
91.	Is access to the general area of the communications facility restricted?	
92.	Have procedures been established to tighten access to a facility as the DEFCON increases?	
93.	Is the security guard force effective?	
94.	Have "tonedown" or camouflage techniques been applied to reduce the site's visibility?	
95.	Is the size of critical components (towers, etc.) as small as possible (consistent with the requirement for reliable communications) to reduce target size?	
96.	Have site personnel been assigned security alert responsibilities and are they trained to perform their responsibilities?	
97.	Are site inspections performed periodically?	
98.	Have supplies for sustained operations independent of normal resupply activities (e.g., adequate stocks of food, water, POL) been properly secured and protected?	