

114532

~~17248~~

BY THE COMPTROLLER GENERAL

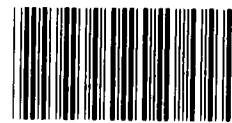
Report To The Congress

OF THE UNITED STATES

Defense Needs Better System For Assuring Adequate Security At Reasonable Cost On U.S. Bases

The Deputy Under Secretary of Defense for Policy Review has authority and responsibility to establish security policy for all military assets, but except for a few sensitive assets, Defense has not taken an active role in managing security programs. The services and local commands design their own security programs to protect all other assets. In view of the enormous cost of protection and the many independent approaches being taken, an established management system within Defense or among the services is needed.

Although Defense planned to address specific security problems identified by GAO, it did not agree with GAO's proposals for strengthening its role in managing security programs. Instead, Defense prefers to continue its incremental approach of providing guidance and of monitoring for a few highly sensitive assets.



114532



PLRD-81-1

MARCH 6, 1981

015860

Request for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760**

Telephone (202) 275-6241

The first five copies of individual reports are free of charge. Additional copies of bound audit reports are \$3.25 each. Additional copies of unbound report (i.e., letter reports) and most other publications are \$1.00 each. There will be a 25% discount on all orders for 100 or more copies mailed to a single address. Sales orders must be prepaid on a cash, check, or money order basis. Check should be made out to the "Superintendent of Documents".



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON D.C. 20548

B-200228

To the President of the Senate and the
Speaker of the House of Representatives

Our report shows that, although physical security is an essential element of national security and the cost of security is quite high, the Department of Defense does not have an effective system for assuring adequate protection at a reasonable cost.

Excluding a few highly sensitive assets, the services and local commanders have been left to independently design and monitor protection systems for all other assets. We believe that this approach has resulted in questionable uses of security equipment and people and that, in some cases, adequate protection may not be provided for important assets.

We are sending copies of this report to the Director of the Office of Management and Budget; the Secretary of Defense; and the Secretaries of the Army, Navy, and Air Force.

A handwritten signature in black ink, appearing to read "Thomas A. Steyer".

Comptroller General
of the United States

D I G E S T

The military services spend enormous amounts annually for people, equipment, research, and for programs to upgrade facilities to maintain physical security of military people and equipment.

Physical security includes three basic ingredients: threat, assets to be safeguarded, and protective measures against espionage, sabotage, damage, and theft. (See p. 1.)

Although the Deputy Under Secretary of Defense for Policy Review has authority and responsibility to establish uniform physical security policy, the Department of Defense and its Physical Security Review Board have not taken an active role in providing guidance, except for a few highly sensitive assets--nuclear and chemical weapons and materials; arms, ammunition, and explosives; and classified information. Protection programs for other items are left to the individual services, and frequently, to local commanders. (See p. 7.)

This has led to parochial interest prevailing in some cases, while in others, to reactions to isolated incidents of theft or sabotage influencing security decisions. This approach does not ensure consistent coverage of similar assets or proper emphasis on the most appropriate assets. The net effect is a possible lowering of security effectiveness and/or the spending of critical funds for questionable protective measures. (See p. 27.)

Because of differing requirements or no requirements, protection programs for similar assets vary widely. To varying degrees, depending on the asset and/or service, base commanders frequently make independent decisions on how to design

protection. Decisions are influenced by requirements; availability of people, money, and equipment; and tradeoffs among the most appropriate protection techniques.

Protection of ordnance storage areas is one example where considerable contrast exists. Fort Bragg, North Carolina, employs contract guards while Camp Pendleton, California, uses marine infantrymen. And even though Fort Bragg's area is larger and it has twice as many storage facilities to protect, it has fewer guard towers, fewer levels of communication, and less than half the number of guards. (See p. 10.)

Another example is arrangements at Fort Belvoir, Virginia, and Cape Canaveral, Florida. Fort Belvoir facilities are antiquated. Some unfenced storage facilities are deteriorated, and door locking hasps on two magazines are inadequate. (The Army began corrective action during GAO's review.) In contrast, Cape Canaveral's storage facilities are modern, equipped with multiple levels of intrusion detection equipment, and have a locking system. (See p. 11.)

Except where Defense or individual services have issued instructions, local commanders must decide whether to use people for protection, or equipment, or a combination of these.

At Cecil Field Naval Air Station in Florida, a computerized card-entry system to control access to hangars and flight-line areas was installed. This system reportedly achieved a payback in 1 year by reducing the number of guards at gates. In contrast, Oceana Naval Air Station in Virginia has given no consideration to more modern or economical methods of controlling entry. (See p. 16.)

Camp Pendleton is considering a \$200,000 closed-circuit television observation system in its ordnance storage area which it believes can eliminate 35 marine guards. Fort Bragg, however, intends to install

interior intrusion detection systems in munitions bunkers but has no plans to reduce its contract guard force. (See p. 16.)

Defense's Office of Security Plans and Programs makes selected site visits in connection with the assets for which it has issued guidance. However, oversight or monitoring of other physical security operations is left to the services.

No specific efforts are being made within Defense or among the services to make sure that proper physical security is provided at a reasonable cost. As a result, protective measures--both people and equipment--at many locations appear unneeded or questionable considering the costs and degree of protection provided.

The Armed Forces Staff College, for example, has 29 armed marine guards. The college compound has two gates, three buildings for student instruction (classified documents are stored in a vault in one building), and a housing area. The vault is equipped with intrusion detection equipment which is monitored during nonduty hours. According to Navy criteria, security for the vault requires six marines, and according to a past Navy personnel review, security for the classrooms requires four marine sentries. (See p. 19.)

Fort Myer, which covers about 240 acres, provides housing for many of the top military leaders in Washington. About 170 military police are assigned to provide security. Some of their duties include (1) roving patrols, (2) a patrol to escort funds, (3) guards at two entrances to log incoming vehicles and to direct traffic, and (4) traffic accident investigations involving nonmilitary equipment even though Army regulations do not require them. (See p. 20.)

In view of the enormous cost of protection, the disparate and independent approaches taken to provide security by services and

bases, and the questionable need for security people and equipment at many locations, an established management system within Defense or among the services would appear to offer opportunities to assure adequate protection at a reasonable cost.

AGENCY COMMENTS AND GAO EVALUATION

The Department of Defense did not agree with GAO's proposals for strengthening its role in managing security programs. Instead, Defense prefers to continue its current incremental approach of providing guidance and of monitoring for a few highly sensitive assets. Defense, while it was sympathetic with and supported avoiding unnecessary costs, believed services' broad guidance covers other assets and that installation commanders should continue to have responsibility and authority to decide on security measures needed in line with the congressional intent of the Internal Security Act.

Defense planned actions to reduce expenditures related to several examples GAO noted, but Defense saw no need for efforts to surface and resolve similar uneconomical conditions.

GAO disagrees that Defense should maintain its current approach because (1) an enormously expensive program exists without a Defense or servicewide organized management system, except for a few highly sensitive assets, (2) opportunities exist to improve security and conserve funds, and (3) the Internal Security Act did not intend to preclude Defense from being involved in how commanders provide protection. In fact, Defense is involved in the security of highly sensitive assets. (See p. 27.)

RECOMMENDATIONS TO THE SECRETARY OF DEFENSE

The Secretary of Defense should establish a management system for effectively

achieving protection at a reasonable cost.
The Secretary should:

- Establish more uniform Defense-wide physical security policies and standards.
- Intensively monitor the services' management of physical security.
- Expand the roles and tasks of the Office of Security Plans and Programs and/or the Physical Security Review Board to include a wider spectrum of physical security matters.

GAO also recommends that the Secretary of Defense direct the service Secretaries to rejustify, substantially reduce, or eliminate the use of people and/or equipment at specific locations. (See p. 28.)



C o n t e n t s

		<u>Page</u>
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
	What is physical security?	1
	The importance of physical security within Defense	2
	Program costs	2
	Objectives, scope, and methodology	4
2	IS DEFENSE ADEQUATELY MANAGING PHYSICAL SECURITY?	5
	Physical security's management principles and elements	5
	Defense and service physical security organizations	6
	Present criteria and guidance for providing protection	7
	How physical security programs are implemented	9
	Oversight/monitoring of base programs	17
3	PROTECTIVE MEASURES AT MANY BASES ARE UNNEEDED OR QUESTIONABLE	19
	Questionable need for and use of security personnel	19
	Questionable need for and use of security equipment	22
4	CONCLUSIONS, AGENCY COMMENTS AND OUR EVALUATION, AND RECOMMENDATIONS	24
	Conclusions	24
	Agency comments and our evaluation	26
	Recommendations	27
APPENDIX		
I	Military installations visited during our review	29
II	Service security organizations, roles, and responsibilities	30
III	Variances in 10 ordnance storage areas	32
IV	Letter dated December 11, 1980, from the Deputy Under Secretary of Defense for Policy Review	33

CHAPTER 1

INTRODUCTION

WHAT IS PHYSICAL SECURITY?

Physical security is:

"That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, and theft." 1/

Physical security incorporates three basic ingredients: threat, assets (objects to be safeguarded), and protective measures. Threats can range from perceived terrorist action to employee pilferage, assets can range from highly sophisticated weapons to shop tools, and protective measures can include any combination of equipment (fencing, alarm systems, lighting) and personnel.

Personnel consist of base law enforcement people and usually specifically assigned interior guards. Either group can include military, or nonmilitary, or both. A law enforcement group provides police services and assists in protecting property and preventing or suppressing crime. This force is usually military and is specifically organized, trained, and equipped to protect the security interest of the local command. Interior guards provide additional security for a specific asset/area. This type of security is usually an ancillary duty and is provided by military people who are not fully trained in security requirements and procedures. For some bases, a military police unit may perform the entire physical security function.

Security management is a major challenge. The likelihood of different threats versus the sensitivity of different assets must be evaluated and translated into a system of protective measures which will provide adequate security at a reasonable cost.

1/Joint Chiefs of Staff Publication No. 1.

THE IMPORTANCE OF PHYSICAL SECURITY WITHIN DEFENSE

Losses or sabotage of military assets are particularly sensitive because such incidents cast doubt on the military's preparedness and on the U.S. defense posture. Thus, adequacy of physical security is a key ingredient in military readiness. But, it is impossible, impractical, and costly to design programs to deal with all perceived threats. In fact, if protective programs are elaborately designed for absolute protection against any scenario, the assets become less readily available when the military itself needs the items.

PROGRAM COSTS

Providing security, law enforcement, and related functions within Defense is expensive. Although its total cost throughout the military services cannot be accurately calculated, enough information is available to indicate that these functions cost around \$2 billion annually.

Each service provided us its total worldwide authorized positions for military and civilian personnel who work full-time in these functions, except for Navy civilian positions which were not available. Using Defense average costs for military and civilian personnel within each service, we estimated 1980 personnel costs. Further, we used a Defense report that contained information on guard services provided by contractors in 1979. On the basis of this data, we found that personnel costs exceeded \$1.8 billion a year, as summarized below:

	<u>Military</u>	<u>Civilian</u>	<u>Contract</u>	<u>Total</u>
	----- (000 omitted) -----			
Army	\$ 491,143	\$26,095	\$20,471	\$ 537,709
Navy	157,070	(a)	13,895	170,965
Air Force	787,196	37,499	3,890	828,585
Marine Corps	<u>264,464</u>	<u>-</u>	<u>-</u>	<u>264,464</u>
Total	<u>\$1,699,873</u>	<u>\$63,594</u>	<u>\$38,256</u>	<u>\$1,801,723</u>

a/Costs are unknown.

These costs, however, are not totally accurate representations of the cost of physical security personnel. The costs are understated for several reasons: (1) the data does not include large numbers of military people who provide security on a part-time basis, (2) the Navy was unable to provide the authorized positions for civilian personnel even though Navy policy is to employ civilian personnel for all security functions which do not require military personnel, and (3) a limited check of the Defense report showing contract costs disclosed that at least one contract valued at over \$5 million was omitted. On the other hand, the personnel cost shown are overstated for several reasons: (1) the data includes personnel in functions not related to physical security, such as correctional personnel, and (2) the data includes law enforcement personnel who may or may not be considered as providing physical security. Also, individual service figures should be qualified because the Marine Corps data, for example, includes marines dedicated to the State Department and some other service activities.

In addition to personnel costs, millions are being spent for equipment procurements, research and development, and security upgrade programs. Some examples follow:

- The Army, Air Force, Navy, and Marine Corps plan to spend about \$45 million in fiscal year 1981 for arms, ammunition, and explosives; security equipment; and facility upgrade programs.
- The Army's research and development program for interior intrusion detection systems, the Air Force's program for exterior intrusion detection systems, and the Navy's program for emergency destruct systems for classified information are estimated to cost \$10.7, \$37.3, and \$1.2 million, respectively, in fiscal year 1981.

Defense and service officials object to the use of the personnel and equipment cost data presented because this report deals with nonsensitive assets at U.S. bases, but the above costs include worldwide security for all assets--including highly sensitive assets, such as nuclear and chemical. It is obvious, however, that (1) total costs for the subjects in this report cannot be accurately calculated, except perhaps for some aspects of the Air Force's program, (2) the cost of physical security among all services is not known to Defense, and (3) the cost of physical security is significantly large.

OBJECTIVES, SCOPE, AND METHODOLOGY

We examined the Defense/service system for providing physical security at continental U.S. military bases. We evaluated the system in terms of whether it would result in adequate base-level protection programs that are configured at reasonable cost.

Our basic approach was to select bases in each service, examine factors affecting the base security program (threat assessments, local plans, personnel types, local management mechanisms) and compare protection of similar assets among bases. Specifically, we examined the protective measures for nonnuclear weapons storage areas, expensive/critical equipment (aircraft, motor pools, flight-line areas), and base life support systems (large petroleum storage areas, power centers, and communications centers).

Our work involved numerous discussions with officials at Defense and service headquarters, some major commands, and 15 military bases. Instructions, plans, audit reports, inspection reports, and similar documentation were examined at all levels of our work. Our site work was fairly intense at eight locations. Seven other locations were added either to obtain a cursory look at overall operations or to get more coverage on specific items. Appendix I contains a list of installations we visited.

CHAPTER 2

IS DEFENSE ADEQUATELY MANAGING PHYSICAL SECURITY?

Defense provides criteria and guidelines for protecting highly sensitive assets--nuclear and chemical weapons and materials; arms, ammunition, and explosives; and classified information. The protection programs for the many other military assets are determined by the individual services, and frequently, by individual bases. Therefore, Defense does not have a centralized system for assuring adequate protection at a reasonable cost, except for some aspects of the highly sensitive assets, even though enormous amounts are spent annually for the protection of the many other assets. To varying degrees, individual services have independently developed programs for managing other assets.

Thus far, Defense has only partially covered the logical management principles (What needs protection? To what degree should protection be provided? What is the best and most reasonable cost way to provide protection?) for the highly sensitive assets. Also, essential management system elements (providing criteria and guidance, properly implementing programs, and obtaining feedback on operations) do not always exist within Defense or collectively among the services. Some elements do exist within some services. The lack of system elements, on a Defense-wide basis, is best illustrated by existing protection measures for the assets for which Defense has not established programs. Some aspects of the highly sensitive programs may also suffer from the lack of a better management system.

If more attention were given to the principles of physical security, along with the establishment of firmer management system elements within Defense or collectively among the services, large opportunities would exist for bringing about adequate protection at a reasonable cost.

PHYSICAL SECURITY'S MANAGEMENT PRINCIPLES AND ELEMENTS

The key management principles governing a sound physical security system should, in our view, address the following key questions:

- What is the threat that determines what needs protection?

--To what degree should the designated assets be protected?

--What is the best and most reasonable cost way to provide protection?

These essential principles have not received sufficient attention for enough military assets or functions. Regarding what needs protection, Defense has reacted to the most sensitive items, and the services have chosen to establish protection programs for only some of the other military assets. Regarding degree of protection, Defense has provided minimum protection criteria for the highly sensitive items and allowed services and bases to independently adopt additional protection measures. Regarding efficiency in protection, Defense generally is silent except for policy statements. For example, in its arms, ammunition, and explosives guidelines, Defense states:

"DOD components shall apply sufficient manpower and funds to AA&E [arms, ammunition, and explosives] physical security programs at all levels in order for progress to be effective and efficient. Systems should incorporate technology and equipment available within the Federal Government and the private sector to provide cost effective protection * * *."

Under the current management system, local commands often apply these principles, but we doubt whether the commands are equipped to deal with all principles.

Besides the principles, a sound management system should include certain essential elements--guidance and criteria, mechanisms to assure guidance and criteria are properly implemented, and monitoring/feedback mechanisms to bring about needed program direction and emphasis (as well as to assure adequate implementation): Generally, except for certain assets, these elements do not exist within Defense or collectively among the services.

DEFENSE AND SERVICE PHYSICAL SECURITY ORGANIZATIONS

Although certain Defense components are tasked with managing physical security, their roles have not been broad enough to deal with physical security as a system. Furthermore, the services have organizational entities with responsibilities for managing physical security, but

depending on the service, the depth of these organizations' roles varies. Also, no concerted structure exists among the services' organizations to deal with common issues except as they pertain to highly sensitive assets.

The Deputy Under Secretary of Defense for Policy Review is responsible for formulating uniform physical security policy. Defense's current philosophy for physical security matters is to exert little control over individual services or local commanders except for the highly sensitive assets (nuclear and chemical weapons and materials and arms, ammunition, and explosives). Accordingly, there exists within the Policy Review organization an office--Security Plans and Programs--which is responsible for policies, standards, and procedures for the highly sensitive assets and for their effective and uniform implementation.

To coordinate servicewide approaches to certain common problems, Defense has a Physical Security Review Board which is comprised of Defense and service headquarters members. Thus far, the Board's efforts, including monitoring, have been limited to nuclear and chemical items and conventional arms, ammunition, and explosives. Recent initiatives have also included communications stations, sensitive drugs/metals, and petroleum.

Security organizations within the services include the Air Force headquarter's Office of Security Police, the Army headquarter's Law Enforcement Division, the Marine Corps' Manpower Plans and Policy Division, and several fragmented elements within the Navy. With these different organizations, the emphasis or approach to managing security is somewhat diverse. Appendix II summarizes these organizations' roles and responsibilities.

PRESENT CRITERIA AND GUIDANCE FOR PROVIDING PROTECTION

Defense has taken a lead role in establishing minimum protection criteria for highly sensitive military assets.

For nuclear and chemical weapons and materials and for munitions, Defense has issued manuals and requirements covering policies, standards, criteria, and procedures for protection. Generally covered are minimum requirements for planning; perimeter security; storage structures and their protection systems; electronic security systems; communications support facilities; security procedures (including personnel requirements); and equipment, training, and transportation. These criteria, and supplemental

service criteria in most cases, are specific enough for monitoring and controlling the adequacy of base-level security for highly sensitive military assets.

Defense emphasizes that the requirements for these assets are minimums and expects each service or base to have more stringent requirements if necessary. For the other military assets, each service decides whether guidelines for protection should be issued and what protective measures should be specified. As a result of this method (1) services have issued differing guidance to carry out Defense's requirements, (2) some services issue guidance on certain assets, whereas other services do not, and (3) in instances where two or more services issue guidance for an asset, the guidance may differ among the services.

The services have issued differing guidance for Defense's requirements for arms, ammunition, and explosives. For instance, Defense requires that its category I munitions, such as sensitive missiles, be under constant surveillance or protected by intrusion detection systems. The services have issued somewhat different requirements covering this aspect of protection for category I munitions. For example:

- The Air Force requires two levels of intrusion detection equipment.
- The Army has issued "mandatory" instructions which parallel Defense's requirements, but it also has stated that "recommended" protection should include intrusion detection equipment without considering the amount of surveillance.
- Navy instructions state that intrusion detection systems may be used if certain facility structural requirements are not met.

The Marine Corps has not issued separate guidance; instead, it uses Defense guidance.

The following table illustrates examples of how one service may issue protection requirements (for assets not covered by Defense) and other services may have no specific requirements for the same asset.

Service Security Requirements for Selected Assets

<u>Asset</u>	<u>Air Force</u>	<u>Army</u>	<u>Marine Corps</u>	<u>Navy</u>
Aircraft	X	X		
Air traffic control facilities	X			
Data processing	X	X		
Funds	X		X	
Petroleum	X	X		
Vehicles		X		
Communications	X	X		X

Furthermore, where more than one service issues instructions for an asset, the instructions may vary. For example, Army requirements for packaged petroleum products include lighting and perimeter protection or guard protection during nonoperational hours. In contrast, Air Force regulations only briefly mention petroleum storage area security but encourage local commands to consider using physical security aids.

HOW PHYSICAL SECURITY PROGRAMS ARE IMPLEMENTED

The existing management system allows large latitudes in how base-level protection programs will be designed and operated. Obviously, where no Defense or service protection requirements exist, bases must independently decide on how to design protection. Further, where requirements do exist, bases have latitudes to exceed requirements, depending on local conditions, or to request approval for not complying. Program operation decisions are influenced by resources available to use for protection. Also, local decisions have to be made on tradeoffs among the most appropriate protection techniques. Given these conditions, it is not surprising that drastic variances exist among the bases in the types of protective measures used.

Local decisions on program operation

Except where Defense has issued guidance or where individual services or major commands mandate protection programs, local commands make many operational decisions. To varying degrees, depending on the asset and/or service, the major operational decisions left to local commands are:

- Numbers of people to use for security. This element seems to fluctuate among different locations depending on the availability of people and the local designation of areas or posts to guard. The areas or posts designated may be dictated by (1) base size, location, and arrangement, (2) base mission, (3) number and mix of security areas, and (4) availability of other protective measures, such as intrusion detection/deterrence equipment.
- Types of people to use for security. People providing security may be military, Government civilians, contract, or combinations of these. Sometimes, service policy overrides local prerogatives. For example, the Air Force generally requires military people to protect highly sensitive assets, the Army states that its military police will not protect nonsensitive assets but may be used for law enforcement, and the Navy uses marine guards in some cases and encourages civilian guards for most duties but states that contract guards will be used only in special circumstances.
- Selection of security equipment. Depending on the local view of asset vulnerability, knowledge of and funding for equipment, and personnel availability, local decisions have to be made on the use of perimeter fencing, lighting, intrusion detection systems; sentry dogs; and the many other equipment deterrence/detection systems.

Different protection programs used

Examples of different protection programs for similar assets among bases are summarized below.

- Protection methods at ordnance storage areas varied considerably. For example, Fort Bragg at one time employed infantrymen but now uses contract guards while Camp Pendleton uses marine infantrymen. And, even though Fort Bragg is larger and it has twice as many storage facilities to protect, it has fewer

guard towers, fewer levels of communication, and less than half the number of guards.

--One of the most obvious contrasts between ordnance storage facilities exist at Fort Belvoir and Cape Canaveral. Fort Belvoir facilities are antiquated. (See photographs on pp. 13 and 14.) Some storage facilities in the south area are deteriorated. The walls are made of hollow tile and can be easily broken or cracked. In the north area, door locking hasps on two magazines are inadequate, allowing possible forced entry. Further, these two magazines are not fenced. ^{1/} In contrast, the Cape Canaveral storage facilities are modern structures. (See photographs on p. 15.) They are equipped with two levels of intrusion detection equipment and have a proper locking system. (App. III illustrates more details of variances in 10 ordnance storage areas.)

--Differences occurred in protection of aircraft flight-line areas. For instance, at Simmons Army Airfield (Fort Bragg), 3.7 miles of fence enclose the approximately 300-acre area. The airfield has several hundred aircraft parked outside hangars. A 24-hour gate guard and a one-person patrol (with a sentry dog) within the compound provide security. However, the interior patrol is not a dedicated guard, as required by Army regulations, and is on call for backup assistance anywhere on post. In contrast, at Davison Army Airfield (Fort Belvoir), the parking area is fenced and has 38 military police providing security. During nonduty hours, the 45 nontactical aircraft are parked in hangars within the compound. Defense officials contended that the differences in mission and threats to Simmons versus Davison warranted the different levels of protection. While this could be true, neither location has clearly documented its threat in terms that can be translated into protection requirements. In fact, in 1978, a major mission at Davison was terminated, but the staffing was not reduced.

^{1/}During our audit, the Army replaced the defective hasps and plans to fence and consolidate munitions into new structures. During the interim period, guard checks of the bunkers have been increased to one every hour.

--At Cherry Point, a large underground aviation gas storage area has lighting and posted signs but is not fenced. In contrast, Fort Bragg's aviation gas storage area is located within the fenced airfield and has another fenced enclosure for the underground storage area. This inner area had lighting and entry controls and is a checkpoint for the airfield military police patrol.

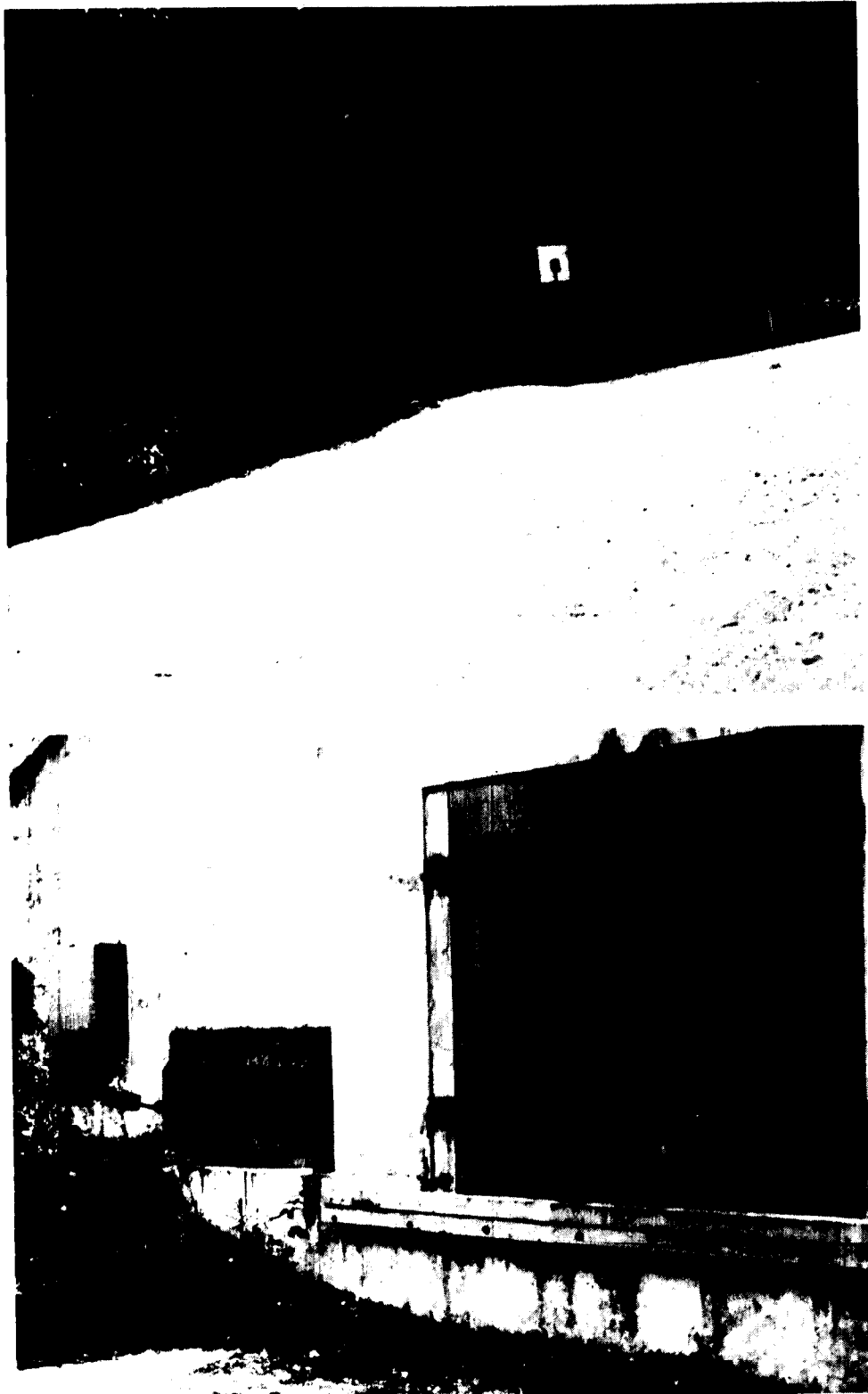
--At Camp Pendleton, the motor pool was equipped with perimeter lighting. However, the lights were removed because of an energy conservation program. Yet at Fort Bragg, the motor pool lighting was cited as being inadequate, and consequently, additional lighting was installed.

--At Fort Belvoir, military police provide escorts for all funds transports regardless of amount. In contrast, Cape Canaveral and Fort Bragg provide fund escorts only for amounts generally over \$2,000.

In addition, the protective measures provided for important assets sometimes are less than the protective measures provided for less important assets. For example, Davison Army Airfield installed intrusion detection equipment following the theft of an air-conditioning unit at its marker beacon facility in Maryland, while its primary navigational air facility at Fort Belvoir has no such protection equipment even though it is located on a remote area of the airfield. Army officials disagreed with this example. They commented that the difference in protective measures between an unguarded off-post marker beacon and navigation facilities located on a guarded airfield is certainly understandable. However, the primary navigational facility--an instrument landing system--is not under constant surveillance, is next to a public road, and if damaged, could prevent aircraft landings in bad weather. Furthermore, the marker beacon in Maryland is only a secondary navigational aid, and the response time to its alarm is too long to apprehend any intruder. Thus, we believe it would have been more prudent to install an alarm in the instrument landing system.

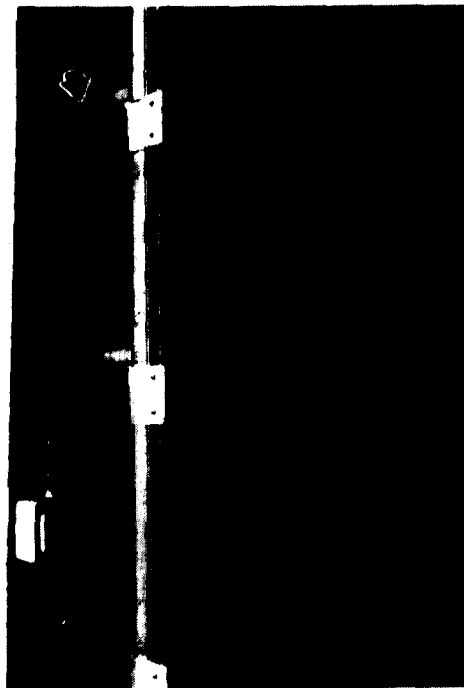
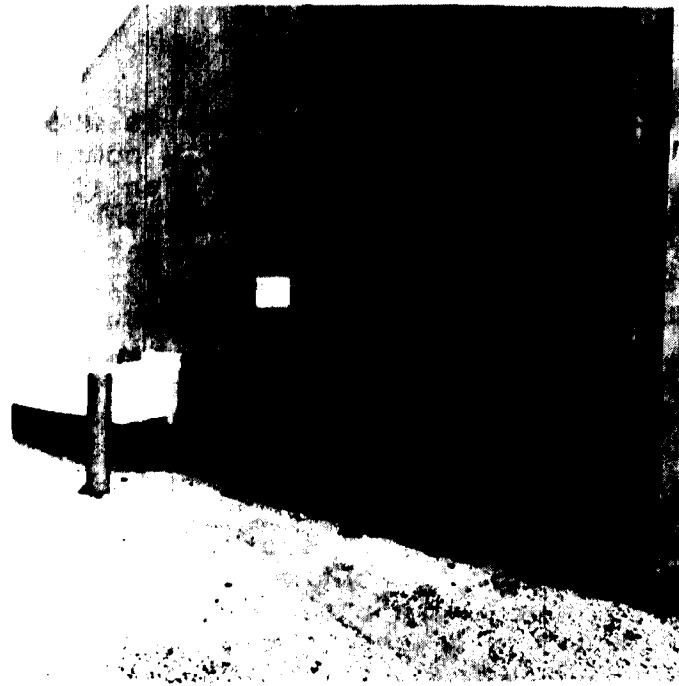


ORDNANCE STORAGE BUILDING AT FORT BELVOIR'S SOUTH AREA
(COURTESY OF THE U.S. ARMY)



A MAGAZINE AT FORT BELVOIR'S NORTH ORDNANCE AREA

(COURTESY OF THE U.S. ARMY)



CAPE CANAVERAL'S ORDNANCE STORAGE FACILITIES ARE MODERN STRUCTURES AND EQUIPPED WITH 1) TWO HIGH SECURITY PADLOCKS, 2) PHONES TO COMMUNICATE WITH SECURITY POLICE, 3) MAGNETIC INTRUSION DETECTION SWITCHES, 4) INFRARED INTRUSION DETECTION SYSTEMS (SEE ARROW), AND 5) INTERIOR DURESS SWITCHES

(COURTESY OF TECHNICOLOR, INC.)

Tradeoffs among
protective measures

A major decision in protection programs is whether to use people for protection, or equipment, or a combination of these. Two general schools of thought exist on the use of security equipment. Some believe equipment reduces the need for security personnel; others believe equipment merely improves the effectiveness of security personnel. Our observations show that either condition may result.

Except where Defense or higher commands mandate protection measures, local commanders have to make tradeoff decisions between equipment types and personnel without the benefit of others' experiences. For example:

--Cecil Field Naval Air Station installed a computerized card-entry system to control access to hangars and flight-line areas. This system reportedly achieved a payback in 1 year by reducing the number of guards at gates. In contrast, Oceana Naval Air Station has given no consideration to more modern or economical methods of controlling entry.

--Camp Pendleton is considering a \$200,000 closed-circuit television observation system in its ordnance storage area which it believes can eliminate 35 marine guards. 1/ Fort Bragg, however, intends to install interior intrusion detection systems in munitions bunkers but has no plans to reduce its contract guard force.

Opportunities for analysis appeared obvious at other locations visited. These included (1) personnel directing traffic, while other locations used traffic lights, (2) personnel providing visitor information service, while others posted signs designating phone numbers to call for information, and (3) a range of automated entry control or denial systems, while others used personnel.

Many of the equipment aids are rapidly emerging in technology and it is cumbersome, at best, to leave such

1/In discussing this matter with Marine Corps headquarters, we were told that the Marine Corps probably could not afford to approve any large equipment request from Camp Pendleton for its ordnance area.

ingenuity to the many local commands. Air Force officials stated it is initiating training for resources protection personnel and is inviting other services to participate. This and more concerted guidance for local commands would be desirable.

OVERSIGHT/MONITORING OF BASE PROGRAMS

Defense's Office of Security Plans and Programs makes selected site visits for security of nuclear and chemical arms and materials and of arms, ammunition, and explosives. However, oversight or monitoring of other physical security operations is usually left to the services. This, and the lack of interchange among the services, could contribute to instances of underprotection, overprotection, and/or funds applied to protect the wrong assets.

Defense could use several existing mechanisms to monitor operations, but as discussed below, these mechanisms have their limitations.

The Defense Audit Service, the services' audit agencies, and inspector generals periodically review aspects of base-level security. However, the Office of Security Plans and Programs normally does not request Defense Audit Service reviews other than for assets on which it has issued guidance. Furthermore, the individual service audit reports and inspector general reports are not always provided to Security Plans and Programs or the Physical Security Review Board. Also, most audits and inspections are compliance-type, and therefore, would not readily reveal differences in service or command requirements.

Uniform requirements exist for the services to report (1) missing, lost, stolen, or recovered weapons and (2) serious incidents, such as acts of terrorism, large losses or thefts, or major crimes. These reports are made available to Defense, and periodically, to the Physical Security Review Board. Although one Defense official stated Defense uses this information to make program adjustments, the Department primarily uses the information as a base for responding to congressional interests or the media.

All services, except the Marine Corps, require each base to prepare a physical security plan. Air Force plans appeared fairly comprehensive in terms of threat descriptions, coverage of base assets, protective measures, and detailed

descriptions of how to deal with different threat/incident scenarios at each base. Generally, the Army and Navy plans appeared to be collections of operating procedures. Further, some Army and Navy plans were also deficient regarding coverage of all base assets or tenants.

To obtain estimates of the cost of physical security, we had to contact each service. And, as discussed on page 3, some of the service estimates had deficiencies. Further, the cost for the program is not visible in budgets. Rather, physical security costs are in military personnel requests, operation and maintenance, and military construction, and generally are without separate identity as physical security.

CHAPTER 3

PROTECTIVE MEASURES AT MANY BASES

ARE UNNEEDED OR QUESTIONABLE

The cost of people and equipment involved in security is enormous. However, Defense's lack of adequate management of physical security (see ch. 2) results in no specific Defense-wide efforts to provide proper physical security at a reasonable cost. As a result, protective measures--both people and equipment--at many locations appear unneeded or questionable considering the costs and degree of protection provided. Some of the situations were caused by local judgments which did not necessarily include tradeoff decisions on minimum cost versus effectiveness of protection.

QUESTIONABLE NEED FOR AND USE OF SECURITY PERSONNEL

The worldwide cost of base law enforcement people and security guards is over \$1.8 billion annually. Coupled with people shortages in the military services and budget constraints, it is especially important that the number of people assigned security duties does not exceed essential requirements and that their duties relate to important functions only. However, at the military bases visited, we noted instances where the need for military people to perform security tasks was questionable. Some examples follow:

--At the Navy's request, the Armed Forces Staff College has 29 ^{1/} armed marine guards for security. The college compound has two gates, three buildings for student instruction (classified documents are stored in a vault in one building), and a housing area. Guards are used at the gates, on exterior roving patrols, and in one building. The only secure area is the vault in the one building, and security is provided during classroom lectures when classified information is presented. The vault is equipped with intrusion detection equipment which is monitored during nonduty hours. According to Navy criteria, security for the vault requires six marines, and

^{1/}In this and other examples in this chapter, the numbers of people mentioned are the total involved to provide security 7 days a week, 24 hours a day.

according to a past Navy personnel review, security for the classrooms requires four marine sentries. Defense did not comment on this case.

- Camp Pendleton has 58 dedicated marine guards to protect the base ordnance storage area. Other protective measures at the storage area include a perimeter fence, lighting, locks, and an emergency telephone, but no intrusion detection equipment. The ordnance officer-in-charge told us that the use of intrusion detection equipment had been considered in the past, but he did not know why it was not approved. Currently, he is considering closed-circuit television cameras at an estimated cost of \$200,000 for improving security effectiveness in the ordnance area. If approved, the ordnance officer believes the guard force could be reduced by 35 marines. 1/
- Davison Army Airfield has 38 military police mostly responsible for guarding 45 aircraft. The aircraft are parked in a fenced area during operational hours and in hangars during off-duty hours. At Fort Bragg, protection for several hundred similar aircraft is provided by one gate guard and a one-person patrol during each shift. The aircraft are parked in the open within a 300-acre fenced area, not in hangars. Davison officials told us that, before 1978, the security force had other duties. When the mission was terminated, however, the number of military police was not reduced. 2/
- Fort Myer, which covers about 240 acres, provides housing for many of the top military leaders in Washington. About 170 military police provide security for this post. Some of their duties include (1) roving patrols, (2) a patrol to escort funds from one location to another, (3) guards at two entrances to log incoming vehicles and to direct traffic, and (4) traffic accident investigations involving nonmilitary equipment even though Army regulations do not require them. The base commander viewed the

1/See footnote on p. 19.

2/Regarding the number of military police at this installation, Defense said that the Army took action last June to gradually reduce the military police company providing support. Defense also said that a review of all missions of the company is ongoing.

primary role of the military police as protecting persons and property on the base and assisting local officials during a civil disturbance on base and at the Arlington National Cemetery. 1/

--The National Defense University, the Inter-American Defense College, and housing for some top military leaders in Washington are located at Fort McNair. Forty-six military police provide security for this post. Also, nine contract guards provide security for the two main buildings of the National Defense University. Further, 16 of the 46 military police serve as liaison with other services and community police, a duty which is not authorized by the Army. 1/

In each of the above instances, we were told that the military people were providing security functions because that is the way it had been done in the past. However, the degree of security being provided does not address the following issues:

--What is the threat?

--What are the security people actually protecting?

--Is the cost of the security force realistic considering the costs of the force and the degree of protection being provided?

--Are the duties of the security force necessary? If so, do they need to be done by people or could some other means satisfy?

--If the duties must be done by people, is the use of military people, as opposed to civilians, the best alternative?

In our opinion, an evaluation of the above examples would show that some of the duties performed by the military security forces are not necessary, could be done with less people, or could be accomplished more economically by means other than people. For example, what is the threat at Fort Myer that requires 170 military police? And, what are the military police protecting? Can 29 armed marines at the

1/See footnote 2 on p. 20.

Armed Forces Staff College be justified on the basis of perceived threat and the significance of the assets at the college?

In addition to questioning the need for an excess military security force, we question the use of contract personnel. Although 40,000 military people are at Fort Bragg, the commander has a \$237,000 contract which provides for 26 guards to protect the ammunition storage area. Fort Bragg converted from military people to contract guards to free soldiers for speciality and unit training. Currently, over 100 military people provide security on a part-time basis for such areas as motor pools and secure buildings. If additional soldiers could be identified that could benefit from part-time guard duty at the ammunition storage area, the cost of the security contract could be saved. However, a top Fort Bragg official believed that the use of contract guards rather than military people was still a desirable approach. Defense said that the contract approach was a local command decision that was cost effective. However, an informal cost comparison was performed showing contracting to cost about the same as use of military people. One concern, apparently not considered, was whether military personnel costs would be reduced by the use of contract personnel.

QUESTIONABLE NEED FOR AND USE OF SECURITY EQUIPMENT

Except for certain highly sensitive assets, Defense generally leaves decisions on what equipment measures to use, such as locks, intrusion detection systems, and lighting and fencing, to service and local command prerogative. We noted several instances where the protective equipment did not appear justifiable considering the costs and the added security that it provided. These conditions evolved from either service requirements or local decisions. Some examples follow:

--In 1978 the Air Force revised its security instructions for munitions storage areas. The revised criteria require two levels of intrusion detection equipment for "very high risk" munitions. Before 1978 an Air Force study recommended upgrading munitions storage areas Air Force-wide. At Cape Canaveral, 13 munition bunkers which contained only "high risk" munitions and which already had fencing, lighting, and guards were upgraded by adding two high security hasps on each bunker, phones to notify

security of authorized entry, intrusion detection sensors (magnetic and infrared), 1/ and interior duress switches.

Defense said that it did not exceed Defense requirements since the system used was a Defense-approved system. Further, Defense believes the sensor unit to be prudent, cost effective, and necessary. Although the cost of the second sensor is unknown, we question the need for it because of the extremely remote odds of one serving as backup for the other. We also question why the Air Force is the only service to require the dual-sensor system.

--After an embarrassing and highly publicized theft of an Army helicopter, the Army ordered more than 8,000 helicopters to be equipped with door and ignition locks. However, several pilots and officials told us that they could steal a locked helicopter within 10 minutes and that the locking system does nothing to prevent sabotage or malicious destruction to the aircraft since maintenance access doors and other sensitive features are on the exterior. Furthermore, the Army is the only service to require door and ignition locks on helicopters.

--The munitions bunkers at Fort Bragg are fenced, lighted, locked, and under constant surveillance. These conditions satisfy Defense requirements. However, in 1985 Fort Bragg plans to install an intrusion detection system in several munitions bunkers.

Defense said that current plans are to spend \$16,000 for four bunkers--not \$132,000 for all bunkers as planned during our visit. Besides the fact that our inquiries may have prompted the \$116,000-reduction, we question whether any intrusion detection equipment is needed since the four bunkers are under constant surveillance and no plans exist to reduce people.

A critical concern in the above cases is whether the services should commit large sums of money for protective measures that may add little or nothing to the security of the assets the services are trying to protect. Also, could the moneys spent or planned for these projects be better used for more serious security problems?

1/See photographs on p. 15.

CHAPTER 4

CONCLUSIONS, AGENCY COMMENTS AND OUR EVALUATION, AND RECOMMENDATIONS

CONCLUSIONS

Although Defense spends enormous amounts annually for physical security of U.S. bases, no organized management system exists within Defense or collectively among the services to achieve the desirable goal of assuring adequate protection at a reasonable cost. The Deputy Under Secretary of Defense for Policy Review has authority and responsibility to establish uniform physical security policy. However, Defense and its Physical Security Review Board have involved themselves only in physical security of nuclear and chemical weapons and materials and conventional arms, ammunition, and explosives. Therefore, protection programs for other items have been left to the individual services, and frequently, to local commands.

Because of the enormous cost of protection, the disparate and independent approaches taken to provide security by services and bases, and the questionable need for security people and equipment at many locations, an established management system within Defense or among the services would appear to offer opportunities to assure adequate protection at a reasonable cost.

Important principles in achieving the physical security goals would, in our opinion, include addressing the following key questions:

- What is the threat that determines what assets/functions need protection?
- To what degree should designated assets/functions be protected?
- What is the best and most reasonable cost way to provide the proper protection?

Currently, these principles are only being partially addressed. Furthermore, normal management system elements--providing guidance and criteria, assuring proper implementation, and monitoring--do not exist within Defense or among the services except to a limited degree for certain highly sensitive assets.

Given the present state of lack of concerted management, services and bases independently design protection programs. In doing this:

- Services have issued differing guidance to carry out Defense requirements. Some issue guidance on assets not covered by Defense while others do not, and guidance among services covering similar assets vary in protection requirements.
- Program implementation, as well as design and operation, is a decision primarily left to local prerogatives which are influenced by local resources available, such as numbers and types of people, and by equipment to use for security.
- Judgments on tradeoffs between protection measures (usually people versus equipment) are left to local ingenuity except in those instances where services have mandated protection program requirements.

The result of this method is that drastic variances exist among protection programs for similar assets and/or protective measures provided for important assets sometimes are less than those provided for less important assets. Currently, Defense has no way of knowing these conditions due to its lack of monitoring or feedback on operations. Again, the function is primarily left to the services and, with the lack of interchange among services, contributes to unwarranted disparities in protection.

Especially needed in the current environment is attention to economies in operation. Yet, in our opinion, the current management system results in inadequate attention for the need to provide security at a reasonable cost. The fact is that local prerogatives usually prevail in the decisionmaking process to decide what should be protected and by what means the protection will be done. This condition has led, in our opinion, to security people performing relatively unimportant functions and to questionable use of security equipment at some locations. Obviously, a closer look is needed at how security people and equipment are being used and whether they are really needed. We

have already raised questions in an earlier report 1/ about the Army's identifying, monitoring, and reporting its resource needs. However, Defense questioned whether more frequent headquarter reviews would be cost effective. We believe just the Army examples of security personnel use, identified in this report, should prompt more headquarters reviews of Army personnel use.

Overall, we believe that the extent to which base commanders have to use their own prerogative has led to parochial interests prevailing in some cases, while in others, to reactions to isolated incidents of theft or sabotage influencing security decisions. This approach does not ensure consistent coverage of similar assets or proper emphasis on the most appropriate assets. The net effect is a possible lowering of security effectiveness throughout the services and the spending of critical funds for questionable protective measures.

AGENCY COMMENTS AND OUR EVALUATION

We made several proposals to Defense to establish a management system for strengthening its role in managing security programs. Defense did not agree. Defense stated that it has issued several manuals and directives for some highly sensitive assets and is gradually expanding its guidance to cover certain other highly sensitive assets. Defense believed that its incremental approach has resulted in meaningful improvements and proposed to continue this approach.

Defense, while it was sympathetic with and supported the objective of avoiding unnecessary security costs, believes that each of the services has issued policy guidance dealing with other property and assets within its control but which also permits flexibility from command to command. Further, Defense stated that the Congress, in enacting section 21 of the Internal Security Act, intended that a military commander have broad authority and that it would be presumptive in face of this law for Defense to nullify the responsibility and authority of the commanders as to how to protect their installations. In addition, Defense believed that centralizing security guidance standards and requirements at the Defense level for a wide variety of noncritical items would be "micromanagement."

1/"The Army Continues to Have Serious Problems Identifying Its Resource Requirements," (LCD-80-67, June 30, 1980).

Regarding the services' security performance, Defense stated that it monitors those assets for which it has established standards and will continue to monitor any additional assets.

We disagree that Defense should maintain its current incremental approach of providing guidance and of monitoring for highly critical assets. We believe our work clearly shows that, except perhaps for a few highly sensitive assets, Defense does not know whether the services are providing adequate security at reasonable costs. The security provided for many assets, including some for which Defense has issued minimum standards, varies significantly among and within the services. While different security measures are not necessarily bad, the different measures discussed in this report usually were not based on different threats or local conditions. Rather, they resulted from service requirements or local judgments. Furthermore, Defense's current approach--which it proposed to continue--has resulted in protective measures which appear unneeded or questionable, considering the costs and degree of protection provided.

In addition, we do not agree with Defense's view of congressional intent on the Internal Security Act. The Secretary of Defense or commanders designated by the Secretary are authorized to issue regulations. We believe that the Congress did not intend to preclude Defense from getting involved in seeing that commanders protect their property effectively and at reasonable costs. In fact, Defense is involved in the security of several highly sensitive assets.

RECOMMENDATIONS TO DEFENSE

We recommend that the Secretary of Defense establish a management system for effectively achieving protection at a reasonable cost. The Secretary of Defense should consider:

- Establish more uniform Defense-wide physical security policies and standards.
- Intensively monitor the services' operation and management of physical security to ensure a more economical and efficient program.
- Expand the roles and tasks of the Office of Security Plans and Programs and/or the Physical Security Review Board to include a wider spectrum of physical security matters. These roles and tasks should include determining what factors should be considered in tradeoffs

among protective measures; whether the individual services' overall management structures are appropriate; and whether base-level security plans should be more uniform, formally documented, and reviewed by services' major commands and headquarters.

We also recommend that the Secretary of Defense direct the service Secretaries to rejustify, substantially reduce, or eliminate the

- marine guards at the Armed Forces Staff College;
- Army military police at Davison Army Airfield, Fort Myer, and Fort McNair;
- Air Force's installation of any additional dual intrusion detection sensors in conventional munitions storage areas;
- civilian guard contract at Fort Bragg's ordnance storage area;
- planned installation of intrusion detection equipment at Fort Bragg's ordnance storage area; and
- installation of door and ignition locks on Army helicopters.

MILITARY INSTALLATIONS VISITED DURING OUR REVIEWPrimary sites

McClellan Air Force Base
California

Patrick Air Force Base/
Cape Canaveral Air Force Station
Florida

Fort Belvoir
Virginia

Fort Bragg
North Carolina

Marine Corps Air Station
Cherry Point, North Carolina

Marine Corps Base
Camp Pendleton, California

Mare Island Naval Shipyard
California

Naval Air Station
Oceana, Virginia

Additional sites

Langley Air Force Base
Virginia

Pope Air Force Base
North Carolina

Fort Myer
Virginia

Fort Story
Virginia

Naval Air Station
Norfolk, Virginia

Armed Forces Staff College
Virginia

Fort McNair
Washington, D.C.

SERVICE SECURITY ORGANIZATIONS,
ROLES, AND RESPONSIBILITIES

AIR FORCE

The Air Force headquarter's Office of Security Police is a single focal point for planning, directing, and supervising security programs. Emphasis is passed downward through major commands and each base is to have formal plans, a review board, and a security police unit. The police protect critical assets. Each installation's Chief of Security Police is responsible for base plans and compliance inspections.

ARMY

The Army's security program is assigned to its headquarter's Law Enforcement Division which is responsible for establishing policies and standards. Other Army agencies have functional responsibilities, such as research and development. Also, the Army has at its headquarters a Physical Security Review Board, and bases are encouraged to have similar review committees. Local commanders are responsible for all assets under their control and rely on base military police and departments/tenants for security. Further, each base is to have a physical security officer, generally under the base Provost Marshall and separate from the law enforcement functions, who prepares security plans and makes compliance inspections.

NAVY

The Navy has no central organization for security. Several Navy components have criticized this arrangement. Instructions do require bases to have security officers, plans, and review committees. However, the Navy "program" is merely a collection of functions from suborganizations and is not integrated or complete. At base levels, security responsibilities are also a mere collection of functions from various departments and tenants, and personnel responsible for providing physical security generally are from these owning units. However, small police organizations exist primarily under the host command.

MARINE CORPS

The Marine Corps' Manpower Plans and Policy Division is responsible for security. The basic security guide for Marine Corps local commanders is the Navy's physical security manual. Base commanders are responsible for assets under their control. They rely on their military police for law enforcement and security inspections and/or on those infantrymen serving as interior guards for specific asset protection. The Marine Corps does not require base security plans or committees.

VARIANCES IN 10 ORDNANCE STORAGE AREAS

Activity	Sensitivity of item (note a)	Guard type	No. of guards	Physical security measures									
				Detection equipment	Con-trolled area	Entry pro-cedure	Peri-meter fence	Area light-ing	Vault door locks/hasps	Watch-tower	Sentry dog	Auxil-ary power	
Camp Pendleton	I-IV	Military	58	-	-	X	X	X	X	X	X	-	-
Fort Bragg	I-IV	Contract	26	b/X	X	X	X	X	X	X	X	-	X
Cherry Point	I-IV	Military	12	-	X	-	X	-	X	X	-	-	-
McClellan	I-IV	c/Civ./mil.	0	X	X	X	X	X	X	X	-	-	-
Oceana	II-IV	Civ./mil.	3	X	X	X	X	X	X	X	-	-	-
Fort Belvoir (north)	II	Civilian	3	-	X	X	X	X	X	X	-	-	-
Cape Canaveral	II-III	Contract	1	X	X	X	X	X	X	X	-	-	-
Fort Belvoir (south)	III	Military	1	-	X	X	X	X	X	X	-	X	-
Patrick	III-IV	c/Military	0	X	X	X	X	X	X	X	-	-	-
Pope	III-IV	c/Military	0	X	X	X	X	X	X	X	-	-	X

a/Defense categories for arms, ammunition, and explosives. (Category I is most sensitive, while category IV is least sensitive.)

b/Inoperable intrusion detection equipment.

c/No interior guard force; only base police patrols.

THE DEPUTY UNDER SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301



POLICY REVIEW

DEC. 11, 1980

Mr. R. W. Gutmann
Director, Logistics and
Communications Division
General Accounting Office
Washington, D. C. 20548

Dear Mr. Gutmann:

This letter is in reply to your draft report titled, "Defense Needs a Better System for Assuring U.S. Bases Have Adequate Security at a Reasonable Cost," which was transmitted to the Secretary of Defense by your letter dated November 12, 1980. (947389) (OSD Case #5562)

The Department of Defense appreciates the opportunity to provide comments relating to the draft report. The comments submitted include inputs obtained from the military departments.

We would point out that as late as 1974 DoD level standardized security requirements existed only for classified information. Since that time, DoD has established standardized requirements applicable throughout the Department of Defense for critical and particularly important items as follows:

July 1975	Published the Nuclear Weapon Security Manual.
April 1978	Published DoD Directive 5210.63 which established security standards and requirements for nuclear reactors and special nuclear materials.
June 1978	Published the DoD manual which established physical security requirements for sensitive conventional arms, ammunition, and explosives
February 1979	Published DoD Directive 5210.65 which established standards and criteria for the protection of chemical agents.

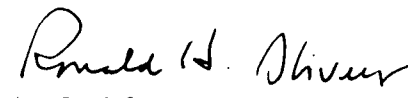
In addition, we are preparing a manual that will provide security guidance for the protection of the Defense Communications System. We are also currently preparing a DoD directive that will establish security and storage requirements for drugs, drug related items, precious metals, and high value and high technology items. We feel this incremental approach has resulted in meaningful security improvements and we propose to continue such an approach since it permits us to focus on very important assets, and potential problem areas as well as to seek out areas that impact similarly on all services.

While the Department of Defense is sympathetic with and supports the objectives of avoiding unnecessary security costs, we would point out that each of the services has issued policy guidance dealing with the security of other property and assets within its control but which also permit flexibility because circumstances vary from command to command. Further, in enacting section 21 of the Internal Security Act, Congress intended that a military commander have broad discretionary authority to establish regulations and issue orders for the protection of property and other assets located on installations under his command. It would seem presumptive in the face of this law for DoD to abrogate the responsibility and authority of commanders to exercise their best judgment as to how to protect their installations and how to allocate their resources for this purpose. In addition to centralize security guidance, standards and requirements at DoD level for a wide variety of noncritical items, in our judgment, would be micromanagement.

The Services security performance is monitored by DoD for those assets for which it has established security standards through reporting requirements and by oversight visits. It will continue to do so including any additional assets for which security standards may be established in the future.

We are attaching specific comments pertaining to the contents of the draft report as enclosures to this letter. We are most pleased to have your personnel conduct this review and believe we in DoD will benefit from their observations and comments.

Sincerely,


for Daniel J. Murphy
Admiral, USN (Ret.)

Enclosures (See GAO note below.)

GAO note: The enclosures contained clarifying language, and we made changes where needed.

AN EQUAL OPPORTUNITY EMPLOYER

**UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548**

**OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300**

**POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE**



THIRD CLASS