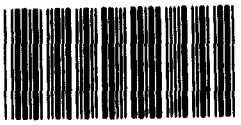

UNITED STATES GENERAL ACCOUNTING OFFICE
Washington, D.C. 20548

FOR RELEASE ON DELIVERY
Expected at 10:00 a.m.,
Wednesday, December 8, 1982

Statement of

Werner Grosshans, Deputy Director

Procurement, Logistics, and Readiness Division

before the

House Armed Services Committee

Investigations Subcommittee

Mr. Chairman, I am pleased to appear before the Investigations Subcommittee to discuss our followup work on the Department of Defense's system of managing physical security at U. S. military bases. We will discuss actions taken by Defense on the recommendations in the Subcommittee's November 5, 1981 report; the recommendations in our March 6, 1981, report, and base entry procedures.

OVERVIEW OF DEFENSE'S POSITION ON SUBCOMMITTEE RECOMMENDATIONS

Defense has ongoing or planned actions intended to address several of the recommendations in the Subcommittee's November 1981 report. In many cases the actions are in the planning stage or have not been fully implemented. Thus, it is not possible to fully evaluate Defense's efforts to improve physical security at military installations.

The major actions are:

--Establishing a Joint Security Chiefs Council responsible for coordinating joint-service security and law enforcement matters; identifying common security problems; promoting consistency in the services' approaches to similar problems; and recommending solutions to these problems.

--Drafting a joint service directive which provides for uniform security procedures for base entry, aircraft, fuels, and communications and automatic data processing equipment.

--Requesting the services to include staffing and physical security costs in their fiscal year 1983 (revised) and fiscal year 1984 budget requests.

Regarding the recommendations aimed at strengthening Defense's roles in the overall management of physical security, Defense believes that its proposed actions plus the existing physical security plans, programs, and procedures will satisfy

the intent of the Subcommittee's concerns.

We are encouraged by Defense's actions to date, however, we believe that much remains to be done if physical security is to be accomplished effectively and economically. I would like to comment briefly on what we think remains to be done.

The most important action that Defense needs to take is to expand its role in providing guidance and direction to the services and then following up to insure that the services' physical security programs are effective and economical and accomplish common objectives. The Joint Security Chiefs Council and the proposed joint service directive are steps in the right direction. However, it is still too soon to determine the effectiveness of these actions because the Council has just recently been formed and has had only a few meetings and the joint service directive is still in draft form.

Defense's effort to accumulate total physical security costs is also a positive step. However, Defense has not provided clear guidance and direction to the services on what costs should be included or excluded, how time should be allocated for persons who perform law enforcement duties as well as physical security duties, or how overhead and equipment costs should be allocated.

Other areas in which Defense could assume a stronger role include expanding the areas covered by incident reporting and establishing OSD physical security inspection teams. At present,

incident reporting to Security Plans and Programs is restricted to matters relating to chemical and nuclear materials and weapons and arms, ammunition, and explosives. For Defense to be in a better position to formulate uniform security policy and guidance, the spectrum of areas covered by incident reporting needs to be expanded. Such additional areas could include flightline incidents, lost or stolen funds, and lost or damaged tactical vehicles and sensitive military equipment where malicious intent is suspected.

The use of OSD physical security inspection teams would also improve Defense's ability to formulate uniform policy and guidance. At present, security inspections are primarily a service responsibility. Consequently, they are conducted from an individual service perspective. Thus, opportunities are not optimized for contrasting and comparing service approaches and selecting the most effective and economical approach.

A more detailed discussion of the above areas, as well as other areas where Defense could strengthen its role in physical security matters, is presented in attachment A.

Next, I would like to briefly discuss Defense's actions on the recommendations in our March 1981 report. Our first recommendation, which was aimed at improving physical security on a Defense-wide basis, was amplified by the Subcommittee's

eight recommendations. For that reason, I will restrict my comments to our other recommendations.

STATUS OF GAO'S RECOMMENDATIONS DIRECTED AT SPECIFIC SITES OR SERVICES

We recommended that the services rejustify, substantially reduce, or eliminate what seemed to be excessive personnel at several installations and unique equipment requirements in the services.

The Armed Forces Staff College, Norfolk, had 29 Marine guards. This number has now been reduced to 21 because of a new Navy regulation which prohibits marines from patrolling housing areas and the Marine Barracks Commander's view that several other patrol areas were not necessary.

The 277 Army Military Police at Davison Army Airfield, Fort Myer, and Fort McNair seemed excessive in terms of what they were protecting. The Army now plans to reduce this number by 30 by the end of fiscal year 1983.

The Air Force's requirement for two levels of sensors in conventional munitions bunkers is contrary to the other service's requirements, the other services have not adopted such stringent security measures. The Air Force is considering less frequent use of such sensors, but still contends that dual level sensors offer the best security.

At the time of our last report, Fort Bragg had 26 contract guards for its munitions storage area. The contract guard force

seemed questionable in view of the large number of military police available. Fort Bragg still maintains that the contract guard force is cheaper than using military personnel and allows military personnel more training time.

We also questioned the need to install intrusion detection systems in some of Fort Bragg's munitions bunkers since they were under constant surveillance by the contract guards. Fort Bragg still plans to install intrusion detection devices and told us that the guard force size would be reevaluated, on the basis of the perceived threat, after the devices were installed.

The Army still requires door and ignition locks on all helicopters, yet no other service requires such locks.

We generally consider the individual service actions to be a positive response to our recommendations and are encouraged by the personnel reductions even though they were not as substantial as we had hoped. However, the positions taken on several of these matters again reinforce the fact that the services and installations operate in a highly parochial mode, and more uniformity in physical security management is still needed. For instance, if the Air Force's two levels of sensors are not considered extravagant, should the other services also adopt this requirement? Also, if the Army helicopter locks are considered necessary, why do Navy officials believe they are useless? Our main concerns are that these and similar inconsistencies in other areas will continue without more central guidance and monitoring by Defense.

Next, I would like to briefly comment on base entry procedures at military installations.

BASE ENTRY PROCEDURES

As you know, on November 23, 1981, the Subcommittee requested the Secretary of Defense to provide a description of policies and procedures at each Defense installation concerning the screening of traffic entering and departing these activities and the type, amount, and cost of the resources used to monitor such access. The following points can be made based on the information provided by the respective services.

--The Navy, Air Force, and Defense Logistics Agency use 4,023 security personnel at a cost of $38.5 million to monitor access to military installations.

--The Army uses 2,225 personnel for the same purpose. However, the Army did not provide cost figures.

--All services and the Defense Logistics Agency charge installation commanders with determining and implementing whatever security measures they deem necessary.

--Security procedures and rationale within and between services vary widely.

--The Air Force appears to have the greatest degree of security procedures commonality among its installations.

We recently visited several Army and Navy bases and the Armed Forces Staff College to obtain more details on base

entry procedures and the rationale at each location. Without exception, specific gate entry and security measures are developed locally and approved by the installation commander. As a result, we found differing entrance security measures at virtually every activity. Attachment B describes the specific procedures and rationale at each activity visited. Many of the differences noted cannot be explained on the basis of differing threats, base unique requirements, or local flexibility. The draft joint-service directive is to address base entry, and we cannot speculate on the impact of the directive on these differences.

In closing, our overall view continues to be that because of the importance and cost involved in providing proper security, more management guidance and attention, including periodic feedback, is needed. While Defense has taken steps on some of the recommendations, we feel it is still reluctant to assume a strong management role in physical security, especially in overseeing and monitoring installation programs. Certain actions which Defense is proposing--estimates of cost, more guidance on security matters and actual impact of the Joint Security Chiefs Council--are not yet fully developed or implemented and, therefore, it would be premature to pass final judgment on them. These actions are steps in the right direction and we are encouraged by them. But we believe that these measures will not fully satisfy the Subcommittee's

concerns, and more is needed. We believe these hearings provide a useful forum to focus on the needed actions.

Mr. Chairman, I will be happy to respond to any questions you may have at this time.

ATTACHMENT A

DETAILED DISCUSSION OF VIEWS AND GAO PROPOSALS RELATED TO SUBCOMMITTEE RECOMMENDATIONS

Recommendation 1: The Secretary of Defense should assume full responsibility for physical security inherent in his mandate. Delegation and decentralization of the actual performance of physical security tasks should continue. But the Office of the Secretary of Defense should be involved in the complete spectrum of DOD physical security activities, issues, interests and problems. Management oversight at the secretarial level should include comprehensive policy articulation, effective compliance and reporting mechanisms, official cognizance of security incidents, participation in government-wide efforts to curb the flow of military weapons to the private sector, and concern with planning, programming and budgeting.

In its May 1982 letter, Defense addressed only the incident-reporting mechanisms mentioned in the first recommendation and said the remaining items were covered in its response to the other recommendations. Defense believed current reporting mechanisms were adequate but indicated that additional reporting mechanisms may be developed for other areas as well.

We believe Defense should expand the areas of physical security covered by incident reporting in order that it can formulate uniform security policy and guidance. Such areas might include flight-line incidents, funds lost or stolen, losses/damages of tactical and nontactical vehicles and sensitive military equipment where malicious intent is suspected, and general crime reports--especially involving Government property. However, Defense has chosen not to assume a stronger leadership role. The Office of Security Plans and Programs receives only security

ATTACHMENT A

reports (missing, lost, stolen, and recovered property reports and serious incident reports) from the services for the areas Defense has issued guidance on (chemical and nuclear materials and weapons and arms, ammunition, and explosives). Defense defers to the services to establish reporting requirements for all other security incidents or events, and these requirements often vary. For example, Naval Air Station, Oceana, submits quarterly reports to its next highest command level. In contrast, Fort Story submits monthly reports to its next highest command level. Besides variances in reporting freqencies, the format and level of detail of the reports vary.

Recommendation 2: Extreme variations in security arrangements at military installations result in inadequate security in some cases and extravagance in others. Those differences not warranted by local conditions, service-unique requirements, or for other valid reasons should be eliminated by establishing uniform DOD-wide policies. As one of a number of compliance and reporting mechanisms OSD inspection teams with joint service representation should visit DOD installations.

In a May 1982 letter to the Subcommittee, Defense disagreed with this recommendation. It believed the issues would be adequately dealt with through the proposed joint service directive; existing inspections and reviews performed by Defense, the service audit agencies, and the Assistant to the Secretary of Defense (Review and Oversight); and staff visits by the Security Plans and Programs Directorate. Defense, therefore, plans to continue its incremental approach of providing general guidance rather than detailed guidance and direction on physical security management matters.

ATTACHMENT A

We believe that more is needed and that OSD inspection teams with joint service representation have merit. Although it is not appropriate for us to speculate on the effectiveness of the draft joint service directive, we have observed problems with other Defense directives intended to provide overall guidance on a subject matter. For instance, the Defense directive for arms, ammunition, and explosives sets only minimum requirements for the services. As a result, substantial deviations exist in the degree of protection provided for this important area by the services and installations. For example, the Air Force uses a two-level intrusion detection system, but no other service has adopted such stringent measures. In another case, Fort Belvoir's munitions bunkers contain more sensitive munitions than those at Oceana Naval Air Station. Yet Oceana's bunkers are equipped with alarmed antitampering devices as well as alarmed magnetic door switches, and Belvoir's bunkers have only alarmed magnetic door switches. These varying conditions illustrate that more is needed than issuance of directives to assure adequate protection at reasonable cost.

Also, while many service inspection and audit functions exist, they are generally directed to compliance-type audits, and both sites mentioned in the prior example would probably not be reported as either deficient or extravagant under existing service-unique or Defense requirements.

ATTACHMENT A

OSD inspection teams with joint service representation would offer a good basis to compare and contrast service procedures, select the most effective and economical ones, and eliminate those that are unnecessary. Accordingly, we believe the Subcommittee's recommendation regarding OSD inspection teams should be implemented.

Recommendation 3: Standardized Department of Defense procedures for accounting for manpower and costs associated with physical security should be established. This data should be separately identified in DOD budgets.

Defense stated that it has started a program to identify physical security costs at all its activities. The budget call went out on July 23, 1982, with supplementary instructions on August 19, 1982, asking the services to supply costs on physical security. The definition of physical security provided to the Defense Comptroller is the Joint Chiefs of Staff definition, as follows:

> "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."

While this is an accurate definition, security at installations usually involves a combination of law enforcement or crime prevention, along with "physical security."

Several service officials told us that the costs of physical security could vary widely depending on what is to be included and excluded. Questions which have not been addressed are as follows:

ATTACHMENT A

--How should overhead be allocated?

--How should time be allocated for persons who perform law enforcement duties as well as physical security duties?

--How should equipment costs be allocated?

--How consistent and adequate is the data base that is used to supply physical security costs?

Defense officials acknowledged that further refinement in the information provided by the services would probably be needed.

Recommendation 4: The Office of the Secretary of Defense should take the lead in establishing an entity for transposing the most effective and economical security practices of each Military Department to the others and challenging those practices which are questionable. In this regard, the subcommittee does not consider the Physical Security Review Board, as presently constituted, a suitable medium. The Board meets infrequently and in practice tends to make decisions collegially. As a consequence, the Board --and the scope of OSD physical security supervision--is heavily influenced by the Military Departments which have a vested interest in avoiding expanded central management oversight of their affairs. The Director of Security Plans and Programs must receive and remain sensitive to Military Department advice, but independently decide issues on the basis of what is best for the Department as a whole and the nation.

Defense responded that this recommendation could be satisfied with the issuance of the joint-service directive and distribution of trip reports prepared by the Office of Security Plans and Programs to the services. Other vehicles cited for enhancing the exchange of information included service participation in various physical security working groups.

The proposed joint-service directive prescribes uniform procedures for installation entry control, aircraft security, fuels, and communications and automatic data processing equipment. The Director, Security Plans and Programs, has been briefed on the proposed directive.

Defense also cites Security Plans and Programs' trip reports as a method of cross-feeding information. However, we were told by service security personnel that they did not always receive copies of trip reports on all inspection visits.

In our opinion, merely exchanging information is not going to resolve the problem. What is needed is a central figure/office authorized to direct and enforce needed changes and performing effective followup.

Recommendation 5: The Department of Defense should prescribe a uniform procedure for local commanders to follow in periodically analyzing their security requirements. The procedure should include threat assessment, determination of assets to be protected and the degree of protection required, explicit assessment of alternatives and their costs, and justification of the alternatives selected as the most economical way to provide effective protection.

Defense believes its proposed joint service directive will answer this recommendation. Since the directive is still only a proposal, it does not currently represent the Defense position on this recommendation. Therefore, we cannot comment on the directive's impact on addressing these key issues in the recommendation which need to be covered in a well-managed installation physical security program.

ATTACHMENT A

On the basis of our March 1981 report and our recent followup work, the services and installations do not uniformly consider threat, type of assets to be protected, protection alternatives, and justification for the alternatives selected when determining the type of physical security needed.

For example, several Oceana Naval Air Station officials recently questioned whether the installation of closed-circuit television and guard towers on the flight line would provide a heightened degree of protection unless better trained personnel are available to operate the system.

On the other hand, Air Force's programs for determining physical security needs do consider the threat, type of assets to be protected, and alternative protection measures. The programs, called the Aerospace Systems Security Program and the Resources Protection Program, provide for establishing a protection committee at each base, a base resource protection plan, and a general policy for protecting a wide range of resources. More specifically, the programs contain the essential elements necessary for determining effective physical security; i.e., threat assessment, type of assets to be protected, and alternative measures to achieve the required protection.

We believe that Defense should develop a program similar to those of the Air Force or adopt the Air Force programs as a basic guide to be used by all the services for determining their physical security needs.

Recommendation 6: The Department of Defense should be intimately involved with other responsible agencies in the government-wide effort to curb the flow of military weapons to the private sector.

Defense has reaffirmed its commitment of cooperation with other Government agencies to halt the flow of arms to the private sector. Defense officials said that coordination with other agencies, such as the Bureau of Alcohol, Tobacco and Firearms and the Federal Bureau of Investigation, was generally done by telephone and that pertinent information obtained from these sources was passed on to installation commanders.

According to the semiannual Defense reports on arms, ammunition, and explosives, losses of munitions within Defense have substantially declined over the years. However; we could not determine whether there was, in fact, an extensive flow of military weapons to the private sector. Therefore, we are not in a position to state an opinion on the adequacy of Defense's efforts in this area.

Recommendation 7: Stronger, more effective management of research, engineering, and procurement of physical security systems is needed to ensure expeditious development of required equipment and prompt termination of unpromising, costly programs.

Defense states that the present structure (Physical Security Equipment Action Group, Tri-Service Requirements Working Group, and Security Equipment Integration Working Group) provides adequate review and has been effective in accomplishing program reviews, cancellations, and adjustments.

ATTACHMENT A

Our current followup work indicates that the groups were working well. For example, as a result of the groups' efforts:

--The Army adopted the Air Force standard security system of fence sensors at Seneca Army Depot, New York, rather than developing its own system.

--Tests were conducted on 15 commercial fence sensors in 1981 to determine if available commercial equipment could be used by or modified for Defense use rather than developing new equipment. As a result, five sensors were found to have potential use and are now undergoing final testing.

--A common visual display system was developed for use by both the Army's Facility Intrusion Detection System and the Air Force's Base and Installation Security System.

We also obtained the current status of the Navy's Anti-Compromise Emergency Destruct Program for classified information which the Subcommittee was interested in last year. We found that the Navy had partially implemented the program and was funding future development at an annual rate of $1.3 million. More specific actions and plans are:

--Full scale development of a field portable unit has been completed, and after evaluation by user agencies, competitive bids for the device will be let.

--Final testing is expected to be completed and production begun during the 1984-86 timeframe for destruct devices

ATTACHMENT A

for five-drawer cabinets, magnetic tapes, microfiche, and on-board aircraft information.

--Exploratory development funds will be discontinued after fiscal year 1983 because the technology base will be sufficient to support development of future devices.

Recommendation 8: The Office of the Secretary of Defense physical security staff should be expanded as necessary to undertake the additional responsibilities recommended in this report.

Defense stated that expansion of the physical security staff was not necessary in view of the joint service directive and the decision not to create OSD inspection teams. However, officials stated that an increased oversight of the other subjects in the draft directive could require future staff increases.

Our followup work showed that the Office of Physical and Installation Security, which has cognizance over base security, has actually reduced its staff from five to three personnel. We were told that there were no plans to replace the two personnel.

To fully implement Defense's proposed actions to improve physical security and to provide the necessary central guidance and direction to insure an effective and economical program, Defense may have to increase its staff. However, we believe that the decision to do so should be deferred until Defense determines the direction and scope of its overall program.

ATTACHMENT B

BASE ENTRY PROCEDURES AND RATIONALE AT SELECTED MILITARY INSTALLATIONS

FORT STORY

Fort Story's procedures specify that it should operate as an open post from 0530 to 2400 but revert to a closed installation from 2400 to 0530. There are two entry gates. One is staffed 24 hours, and the other may or may not be staffed (depending on available personnel) during the day and is closed at midnight. Base entry procedures state that persons are accorded free access to the post if:

--They are in military uniforms or present military identification cards,

--Display Fort Eustis, Fort Story, or any other military installation decals on their cars.

However, we found that, generally, everyone was accorded free access to the post.

The primary rationale for gate sentries is to

--insure the orderly flow of inbound and outbound traffic;

--assist motorists with information or directions;

--visually check vehicles for possible violations such as expired decals, State inspection, license plates, improper equipment, drunk or reckless driving, or possession of illegal drugs.

FORT MCNAIR

Fort McNair has three entry gates. The main gate is staffed 24 hours; the remaining two are staffed only during duty hours and are closed thereafter. Access to Fort McNair is controlled. Only authorized vehicles and personnel are allowed entry. This is accomplished through a check of vehicle decals, personnel identification cards, and a visitor pass system. Persons without military decals or identification must present their driver's licenses, state the purposes of their visits, and have their vehicle license numbers recorded. Those considered not to have bona fide business on the installation are turned away. We were told an average of 10 vehicles a day were determined to have no specific business on the installation and were turned away.

The rationale for these procedures is that the installation commander and with the Military District of Washington (MDW) have decided they want to know who is coming on to the installation, and what their business is and to deny access to those not having official business on base. The Commander, MDW, stated these procedures had resulted in

--the safety and well being of high ranking official residents on the post and

--the regular interception of illegal drug trafficking by soldiers and civilians, interception of drunk drivers, and some nonvalid delivery trucks.

ATTACHMENT B

FORT BELVOIR

Fort Belvoir is designated by the Army as an open post. A major U.S. highway (Route 1) bisects the post. There are five primary access points to the installation. The main gate is staffed 24 hours. One other gate is staffed from 0600 to 2200. Three access points are unstaffed but closed during nonduty hours.

The primary rationale for gate sentries is to expedite the tremendous volume of traffic and serve as a source of information to visitors.

According to Army officials, the staffing of gates at Belvoir will be taken over by a contractor or Department of the Army civilians within the next year.

FORT MYER

The MDW Commander decides the level of access control that will be provided at Fort Myer. Entry procedures are similar to those of other MDW installations, such as Fort McNair and Davison Army Airfield. Fort Myer is referred to by MDW officials as an "observed access post." That is, persons can drive through but officials want to know who is there. Therefore, all persons entering without recognized military decals or identification must show civilian identification, state their destinations, and have their vehicle license numbers recorded.

ATTACHMENT B

MDW officials consider controlled access a very high priority. The rationale for such procedures is expressed in terms of exercising police services or police power at entry points. From July 1981 to July 1982, military police reports originating at the three gates to Fort Myer revealed the following.

Drunk driving	36
Possession of marijuana	17
Traffic violation	25
Identification or driver's license discrepancies	15
Other	22
Total	115

Each day about 16,500 vehicles, or over 4 million annually, enter and leave Fort Myer.

DAVISON ARMY AIRFIELD

There are two entry gates to the field. One gate is staffed 24 hours, and the other is staffed during duty hours and closed thereafter. Davison is considered a restricted area, and access is confined to official business only. Vehicle decals, identification cards, or visitor passes are checked. During duty hours, official visitor vehicles' licenses are logged in. At night, all vehicles and personnel passing through the gate are recorded. Security officials at Davison base their rationale for these procedures on:

--The importance of the airfield in supporting classified missions in a contingency.

--The large number of high-ranking officials that pass through the airfield.

FORT EUSTIS

Fort Eustis has one gate. Guard personnel monitor inbound and outbound traffic and insure orderly flow. Generally, guards control access to the post, except controlled access does not apply during the morning, noon, and evening rush hours on duty days. Gate sentries visually check vehicles for possible violations, such as invalid military decals, expired license plates and inspection stickers, etc., and assist motorists with information or directions.

The Fort Eustis Commander uses his prerogative in establishing the gate control procedures at both Fort Eustis and Fort Story. Entry control is used to meet a number of individual base needs as perceived by the provost marshall or base commander. The following examples were provided by base officials:

--If it is believed that drug traffic is rising, gate sentries can be used to conduct random searches of vehicles entering the base.

--There are concerns about the number of soldier vehicle accidents, and the gate sentry can be used to conduct vehicle safety inspections.

--If there is an alarm on base, the gate can be closed until the cause for the alarm is resolved.

ATTACHMENT B

NAVAL BASE AND NAVAL AIR STATION, NORFOLK

There are eight perimeter entry gates to the Norfolk Naval Base and Naval Air Station. Sentries for these gates are provided by the Marine Barracks, Norfolk. The marine guards function under the command of the Commanding Officer, Marine Barracks, and perform duties required by the Naval Base Commander, Norfolk.

No one is authorized to enter or exit perimeter gates until directed by the gate sentry. Entry is controlled by vehicle decals, proper military identification, or authorized visitor passes. Military uniforms in themselves are not accepted as identification.

The primary documented rationale for gate sentries at this installation is for the purpose of

--fulfilling basic physical security requirements,

---assisting persons who have legitimate reasons for entering, and

--eliminating unnecessary delays.

Marine gate sentries at this installation are justified by Navy officials on the basis that their presence is needed to meet classified reaction missions in the event of a contingency. Their use as gate guards is secondary but meaningful, since installation assets require that only authorized access be permitted.

The public is permitted to visit the installation for occasions of national significance or on "Open House" ship visiting weekends.

OCEANA NAVAL AIR STATION

Naval Air Station, Oceana, has two gates manned by sailors. Vehicle entry is controlled by the standard Navy bumper decal. Temporary and visitor passes are used for vehicles not eligible for decals.

The Naval Air Station does not have a perimeter fence. The boundaries of the base consist of partially fenced areas, leased farm areas, areas of dense foliage, and some open areas. The primary rationale for posting sailors at the gates is

--to present a good image to the public,

--to expedite traffic flow, and

--to provide base information and directions.

ARMED FORCES STAFF COLLEGE, NORFOLK

There are two gates to the Armed Forces Staff College. The main entrance is staffed 24 hours, and the other is open only 1 hour in the morning to expedite traffic. Gate sentries are provided by the Marine Barracks, Norfolk.

Entry is restricted to those vehicles with specific Armed Forces Staff College decals or official visitors. Others are be turned away.

ATTACHMENT B

Marine sentries at the gates are justified by the Commander, Marine Barracks, because they provide the security mission of allowing only authorized personnel aboard the Armed Forces Staff College compound. Security personnel at the Staff College support this rationale on the basis of

--the prevalence of classified material aboard the compound and

--the number of high ranking U.S. and foreign officials frequently present at the compound.

In addition, the Marine Barracks Commander stated the sentries support classified reaction force missions in the event of a contingency.