17 June 1980

MEMORANDUM FOR: Chief, Management Staff, ODP

THROUGH: Chief, Engineering Division, P/ODP

25X1

FROM: [redacted] Chief Engineer
Engineering Division, P/ODP

SUBJECT: "Security Requirements for Automated Information Systems Located in Overseas Installations", comments thereon

Attached are Systems Programming Division and Engineering Division comments on the subject document.

25X1

[redacted]

Attachment:
A/S

25X1

[redacted]

16 June 1980

Comments on "Security Requirements for
Automated Information Systems
Located in Overseas Installations"

1. Requirements for semiconductor volatile memory may be over-restrictive (probably makes no difference now, but could affect use of bubble memories in the future). Non-volatile memory is comparable to non-removable storage media.

2. Removability of storage media ought not be an absolute requirement for overseas computers. Technology appears to be moving in the direction of non-removability. Instead, there should be procedures governing how non-removable media is to be handled (e.g. guarded, encrypted, etc.)

3. Page 16 - 17, paragraph 2 refers to system software services. The word "exclusive" is unclear as is the phrase "secure manner".

4. Page 17, paragraph 3 is unclear. [redacted]

ILLEGIB

5. Page 18, paragraph 5.b.1, requires passwords for each file. It is more appropriate to require that access be authenticated by password and that there be mechanisms restricting file access to authorized users.

6. Similarly, in paragraph 5.c, access to the system ought to be controlled by password. Access to restricted files could then depend on the authentication provided during initial signon. It may be appropriate to utilize file passwords for infrequently accessed collections of files. However, requiring separate passwords for each file will increase the likelihood of passwords being compromised.

7. Audit trail requirement (page 19) is too stringent for existing software.

8. The requirement (page 20, paragraph 3) that a security officer be involved in restarting a failed system is impractical.

9. "Security Deviation" (page 20, paragraph 7) should be clarified. Different reactions are appropriate to different situations.

25X1

[redacted]

ILLEGIB

Page Denied

DRAFT

SECURITY REQUIREMENTS

FOR

AUTOMATED INFORMATION SYSTEMS

LOCATED

IN OVERSEAS INSTALLATIONS

DRAFT

25X1

[redacted]

TABLE OF CONTENTS

SECTION

I Purpose

This manual establishes security requirements, standards, and specifications for the protection of word and/or data processing (ADP) systems (hereinafter referred to as automated information processing systems) and information stored in or processed by 25X1 [redacted] information systems located in overseas Stations or Bases (hereinafter referred to as"overseas location(s)".

II Applicability

The security requirements, standards, and specifications established herein apply to all automated information processing systems used at overseas locations. This includes systems which interface with telecommunications services, as well as stand-alone and networked systems. These requirements do not replace or supersede existing minimum requirements established by other directives, but rather establish a base for additional security in the area covered.

III Responsibilities

A. Responsible Headquarters Component

The Headquarters Component having primary responsibility for the proposed site of an automated information processing system in an overseas location shall:

1. Request of the Chief, Information Systems Security Group, (ISSG) Office of Security, the necessary pre-installation security survey of the proposed overseas location.

2. In coordination with the Chief of Station or Base, approve the designation of a qualified ADP System Security Officer for the proposed site.

3. In coordination with the Chief of Station or Base, the assigned Information System Security Officer (ISSO), and other Headquarters components as required, develop an ADP System Installation Plan tailored to the selected Station or Base. (See Paragraph C. below)

4. Submit the developed ADP System Installation Plan to the Chief, ISSG, Office of Security, for final approval. The transmittal document will include a certification that the requirements, standards, and specifications recommended by the pre-installation security survey team and established herein are to be implemented for the Station or Base.

5. In coordination with the designated Information

Systems Security Officer (ISSO), develop Station or Base Emergency Plan documentation for the evacuation and/or destruction of data and program storage media, and system equipment.

B. Overseas Location

The Chief of each Station or Base proposing to use an automated information processing system shall

1. Provide area, space, and any special recommendations to the appropriate Headquarters component for inclusion in the ADP System Installation Plan.

2. In coordination with the Headquarters component, designate an ADP System Security Officer for the Station or Base.

3. Direct the ADP System Security Officer to establish and implement in coordination with the designated Information Systems Security Officer (ISSO), a formal ADP System Security Program to ensure compliance with the requirements established herein for the location's automated information processing system.

C. Information Systems Security Group (ISSG), Office of Security

25X1 The Chief, ISSG, is responsible as the [redacted] ISSO to determine, formulate, interpret, and disseminate policies, and guide the implementation of the security requirements, standards, and specifications within
25X1 [redacted] and its facilities to ensure compliance with applicable Executive Orders and Directives relating to information systems in accordance with DCID 1/16.

The Chief, ISSG, shall appoint an Information Systems Security Officer (ISSO) for each overseas location designated to use an automated information processing system. The ISSO shall:

1. Serve as the security focal point for each assigned automated information processing system.

2. Review the ADP System Installation Plan for each assigned overseas location to ensure that all requirements, standards, and specifications relevant to the proposed installation are implemented. This includes obtaining written certification from the responsible Headquarters component of the satisfactory compliance with these requirements.

3. Submit for approval by the Chief, ISSG, the ADP System Installation Plan established for each assigned overseas location.

4. Obtain approval for the ADP System Security Program from the Chief, ISSG, for each location. This program shall include the complete spectrum of security controls and safeguards for each system in each location. The ADP System Security Program shall be prepared with appropriate input from other Headquarters components having specific areas of interest. These include but are not limited to the responsible Headquarters component, the Overseas Security Support Branch (Office of Security), the Communications Security Division (Office of Communications), and the Technical Security Division (Office of Security).

5. Conduct and/or participate in pre-installation security surveys of each assigned overseas automated information processing site.

6. As appropriate, coordinate reports received concerning each assigned overseas location's automated information processing system with the Overseas Security Support Branch (Office of Security), the Communications Security Division (Office of Communications), the Technical Security Division (Office of Security), and the responsible Headquarters component.

7. Review the ADP System Security Program established for each assigned overseas location for continued compliance with the requirements, standards, and specifications established herein.

8. Schedule and conduct an annual security survey and audit of each assigned overseas automated information processing system.

D. Overseas Security Support Branch (OSSB), Office of Security

The overseas Security Support Branch shall:

1. Interpret, and disseminate policies relating to physical security matters as they pertain to [redacted] automated information processing systems in overseas locations. 25X1

2. In coordination with the designated ISSO, conduct periodic (minimum once every 2 years) physical security surveys of all [redacted] automated information 25X1

processing systems in overseas locations.

3. As appropriate, coordinate all physical security reports received concerning overseas automated information processing locations with the Information Systems Security Group (Office of Security), the Communications Security Division (Office of Communications), the Technical Security Division (Office of Security), and the responsible Headquarters component.

4. As required, participate in pre-installation physical security surveys of proposed overseas automated information processing system locations.

E. <u>Communications Security Division (CSD), Office of Communications</u>

1. Interpret and disseminate policies relating to communications security matters as they pertain to [redacted] automated information processing systems located in overseas locations, including those systems used for telecommunications services. 25X1

2. Conduct TEMPEST testing for all [redacted] ADP Systems located in overseas locations. 25X1

3. As appropriate, coordinate reports received concerning overseas automated information processing system communications security matters with the Information Systems Security Group (Office of Security), the Overseas Security Support Branch (Office of Security), the Technical Security Division (Office of Security) and the responsible Headquarters component.

F. <u>Area Headquarters, Office of Communications</u>

The Area Headquarters shall:

1. Conduct communications security inspections, excluding TEMPEST testing, of all [redacted] automated information processing systems located in overseas locations. 25X1

2. As required, participate in pre-installation security surveys of proposed overseas automated information processing systems.

G. <u>Technical Security Division (TSD), Office of Security</u>

The Technical Security Division shall:

1. Conduct an Audio Countermeasures (ACM) inspection of all automated information processing system locations and all user terminal positions remote from the automated information processing system central processor.

2. Install an approved alarm system in the ADP Facility and all areas remote from the ADP Facility in which user terminals are positioned. ("ADP Facility" is defined in Section IV A).

[redacted] 25X1

IV System Security Requirements

A. Physical Security

1. ADP Facility Location

25X1

All automated information processing system equipment excluding terminals approved for locations remote from a central processor, shall be located within [redacted] controlled space within the overseas location, in an interior room, when possible, and on a floor which precludes access from the outside (hereinafter referred to as the "ADP Facility").

2. User Terminal Locations

All user terminals should be located within the ADP Facility. Recognizing, however, that Station or Base operational requirements or physical restrictions may preclude the installation of all user terminals within the ADP Facility, the following requirements are established as minimum for the location of user terminals in positions remote from the ADP Facility:

25X1

a. All user terminals shall be located within [redacted] controlled space.

b. All user terminals shall be located in alarm protected areas and, when possible, in rooms meeting the criteria for a "secure area". (See Section IV B - Technical Security).

3. ADP Facility Construction Criteria

a. Existing Buildings

An ADP Facility which is to be located in an existing building shall be constructed to meet the existing criteria for a "secure area".

b. New Buildings

[redacted] 25X1

be approved by the Office of Communications.

4. Personnel Access Controls

a. Station or Base

25X1 Approved 24 hour a day [redacted] protection is required at each location in which an ADP Facility is installed. Headquarters will normally not approve installation of an ADP Facility in sites
25X1 lacking the 24 hour approved [redacted] because of the inability to provide satisfactory alarm response.

b. ADP Facility

25X1 Only [redacted] Staff employees who possess an established need-to-know, as determined by the Chief of Station or Base, shall be allowed access to the ADP Facility. If cryptographic equipment or material is installed in the ADP Facility, appropriate Cryptographic clearances are required. (See Section IV Paragraph C5b).

c. Storage Areas

25X1 Only [redacted] staff employees who possess an established need-to-know shall be allowed access to the approved storage area in which data and program storage media are maintained.

5. Data and Program Storage Media

a. Identification/Labeling

1) Demountable data and program storage media (magnetic tapes, disk packs, floppy disks, and cassettes) shall bear an external label to clearly indicate the highest security clasification and/or compartments of the information stored on the media.

2) Card decks shall be marked so as to clearly indicate the highest security classification and/or compartments of the information stored on the deck.

3) Program listings, including program listings on microform, shall be labeled so as to clearly indicate the highest security classification and/or compartments of the information listed.

4) Any punched paper tapes used shall be labeled and marked so as to clearly indicate the highest security classification and/or compartments of the information recorded.

b. Storage

All demountable data and program storage media, when not being used, shall be placed in an approved Class 5 security container. These security containers may be located within the ADP Facility or the Station or Base vault (other than that used for communications facilities) provided the Station or Base vault meets the standards established for an ADP Facility.

c. Open Shelf Storage

ADP Facilities wherein the system does not have removable storage media or where the internal memory is non-volatile, shall only be approved when the construction of the ADP Facility meets the requirements for open shelf storage of the material contained.

d. Transportation

The physical movement of all demountable data and program storage media outside the approved secure area, or between the overseas location's buildings, shall be accomplished in accordance with existing requirements for the movement of classified documents of an equal classification. The prescribed and approved logging and personal accountability procedures shall be used.

e. Logging and Personal Accountability

1) A logging and personal accountability system shall be established and maintained, and shall be based on procedures approved by the designated Information System Security Officer.

25X1 2) [redacted] Staff employees shall be designated and identifiable on an access list to receipt for all classified data and program storage media.

3) The logging and personal accountability system shall include logs for the removal and return of all demountable data and program storage media from and to the approved storage area.

4) The access lists and the logging and personal accountability system shall be periodically reviewed by the designated Information Systems Security Officer to determine their accuracy and currency.

B. Technical Security

1. Audio Countermeasures

An Audio Countermeasures (ACM) inspection will be conducted in the proposed ADP Facility and in all areas remote from the ADP Facility in which user terminals are to be positioned, prior to the operational implementation of any automated information processing.

2. Alarm Systems

The ADP Facility and all areas remote from the ADP Facility in which user terminals are to be positioned shall be equipped with an Office of Security approved alarm system. If the ADP Facility, or any user terminal area, is partitioned into separate areas by wall to ceiling panels, each subdivided area shall have an independent alarm and/or sensor.

3. Procedures - Alarm Activation

[redacted] 25X1

25X1 25X1

b. The [redacted] shall immediately summon the responsible [redacted] officer.

25X1

c. The responsible [redacted] officer shall inspect the alarmed area for evidence of a penetration or attempted entry.

25X1

d. If evidence of a penetration or attempted entry is discovered, the responsible [redacted] officer shall:

1) Fully secure the affected area. If the ADP Facility or area in which a remote user terminal is located cannot be fully secured after an alarm activation, the area shall be occupied by an [redacted] staff employee until the alarm system is restored to service.

25X1

25X1

2) Report the incident, via an IMMEDIATE cable [redacted]

a) Time of alarm activation

b) Area of alarm activation

c) Type of alarm (volumetric or door contact)

d) Condition at the time of alarm activation, ie.

(1) Was there a power failure in the area?

(2) Did alarm function properly when checked following the activation?

(3) Any other information which will assist the Chief, Regional Security Group, to determine whether the information processing equipment affected can be placed back in operation, and when.

3) Maintain the affected area and equipment in a fully secure status until a response is received.

4) Following the response, arrange for the conduct of a full audio countermeasures inspection prior

to placing the area and equipment back into service.

4. Procedures - Alarm Failure

In the event of an alarm failure the responsible 25X1 [redacted] officer shall:

a. Report the incident via a PRIORITY cable slugged 25X1 [redacted]

1) Time alarm failure discovered

2) Area of alarm failure

3) Type of alarm (volumetric or door contact)

4) As much information about the alarm failure as possible to assist the regional security group and or Headquarters to diagnose the failure problem. If repair instructions cannot be provided by cable, a qualified security officer will be sent to the Station or Base either from the appropriate regional group or Headquarters.

b. Obtain appropriate increased guard coverage until the alarm is again operational.

C. Communications Security

1. Equipment Installation

a. General

National Communications Security policy requires that classified information which is transmitted electrically must be protected either by the use of approved cryptographic equipment, or by protected distribution systems. All transmission paths between a remote terminal and the ADP Facility, therefore, must be protected by one of these means if classified information is processed. The Standards for Protected Distribution Systems are contained in National COMSEC Instruction (NACSI) 4009.

b. Power

1) A non-standard power plug and receptable shall be used for all automated information processing system equipment to the selected power outlet to preclude movement of the equipment from its designated installation position.

2) All automated information processing system equipment shall be connected to a ground and that ground shall be made through the ground wire of the AC power cord.

c. Conduit

1) All equipment installations that plan to use a protected distribution system shall be considered for approval on a case-by-case basis.

2) All automated information processing system equipment shall be installed using a dedicated power run housed in ferrous conduit and terminating at its own breaker in the power panel closest to the equipment.

2. Telecommunications Equipment Installatio

a. Standards

Installations of automated information processing system equipment to be used for telecommunications services shall meet the standards defined in the Office of Communications handbooks OCHB-F 10.70.2 (Staff Communications Security General) and National Communications Security Instruction (NACSI) 5203.

3. Telecommunications Signal Lines

a. Criteria

Signal lines connecting the installed automated information processing system equipment to the Station or Base Communications Center, when the equipment is used for telecommunications services, shall meet the following criteria:

1) The signal line must be optically isolated to break the signal line metallic conductors.

2) The signal line must be non-ferrous cable with the shield grounded at the communications facility end only.

4. Emanations

a. All automated information processing system equipment used in overseas locations shall meet the specifications set forth in the National COMSEC/EMSEC Information Memorandum (NACSEM) 5100.

b. All installations of automated information processing system equipment, regardless of mode of operation, shall be in accordance with the NACSI 5203 publication.

c. All automated information processing system equipment installed in overseas locations shall be positioned, where possible, so as to have a three (3) foot area of control which is the three dimensional space surrounding the automated information processing system equipment.

[redacted] 25X1

e. The following minimum installation separation requirements shall apply to all automated information processing system equipment installed in overseas locations.

SEPARATION FROM	MINIMUM DISTANCE
Transmitters/Receivers	3 Feet
CCTV/Tape Recorders	3 Feet
Converters/Oscillators	3 Feet
Black Signal Lines	2 inches
Modems	2 inches
Black Patch Panels	2 Inches
Power Lines	2 Inches
Black Telephones	3 Feet
Step Down Transformers	2 Inches
Black Computer Processors	3 Feet
Voltage Regulators	2 Inches
Outside and Uncontrolled Walls	3 Feet
Intercom Systems	3 Feet
[redacted]	3 Feet

25X1

f. Radios and/or other electrically operated entertainment devices shall not be located in the ADP Facility nor in any room housing cryptographic equipment. Further, radios and/or other electrically operated entertainment equipment shall not be located within 3 feet of any automated information processing, or cryptographic equipment, regardless of the number of intervening walls.

5. Cryptographic Security

a. All cryptographic equipment shall be installed, operated, and maintained in accordance with the procedures issued by the Office of Communications.

b. All cryptographic equipment and all other COMSEC accountable material will be issued to the Station or Base "Communications Facility COMSEC Custodian" by the Central Office of Record (COR). The Communications Facility COMSEC Custodian will, in turn, issue the required material to the Station or Base ADP System Security Officer on a hand receipt which will be updated semi-annually.

D. Information Systems Security

1. System Hardware

Unless a formal waiver is obtained from the Director of Security, the following automated information processing system hardware requirements are established as minimum.

a. All automated information processing system equipment shall be TEMPEST approved.

b. All automated information processing system central processor units shall possess semiconductor volatile internal memory.

c. All automated information processing system equipment shall use removable data storage media (disks, disk packs, magnetic tapes, floppy disks, tape cassettes).

2. System Software

All automated information processing systems which utilize an Operating System shall provide the following exclusive services:

1) Cause all applications programs to load as scheduled.

2) Allocate memory, direct access storage space,

and devices to applications programs.

3) Handle all input/o tput functions related to available and shared resources.

4) Handle all interrupts designated for applications programs in a known and secure manner.

5) Protect itself, and provide an authorization function to permit only approved sets of individuals and programs to be combined for a particular job run.

6) Provide for the production of an audit trail record. (See Audit Trails, Section IV Paragraph D6).

3. Data Files

25X1
25X1

All data files used and/or created during processing shall contain only data records organized for processing [redacted] and/or [redacted] related information.

4. Sanitization/Destruction

a. Policy

The sanitization requirements and procedures established herein do not apply to "Restricted Data" or formerly "Restricted Data" as defined in Section II, Atomic Energy Act of 1954 as amended, and codified at 42 USC, Section 201(y), or to storage media on which COMSEC keying material has ever been recorded. These materials shall be either destroyed or returned to Headquarters in compliance with current directives concerning such materials.

b. Procedures

1) Card Decks, Program Listings, and Paper Tapes

25X1

When no longer needed for the processing of [redacted] data, card decks, program listings, microform, or paper tapes shall be destroyed in accordance with current security approved destruction procedures

2) All Other Data and Program Storage Media

When no longer needed for the processing of

25X1 [redacted] data, or when deemed inoperative, all other data and program storage media (magnetic tapes, floppy disks, tape cassettes, disk packs, or other rigid magnetic storage devices) shall be either destroyed in accordance with current security approved destruction procedures, or returned to the Responsible Headquarters component via classified pouch for appropriate disposition.

5. System Access Controls

a. Remote Terminal/Terminal Areas

1) User terminals located in positions/areas remoted from the ADP Facility shall be system identifiable, by location, and individually designated for a specific security classification access level.

2) Access to areas in which remote terminals are installed shall be restricted during processing operations; only those terminals designated for the security classification access level being processed shall be logically connected to the data processing system, and only those [redacted] 25X1 employees with an established need to know shall be allowed access to the system.

b. Data Files

25X1 1) Each [redacted] data file shall be controlled by a file password and indicators to describe to the system the type of access authorized.

2) Access to the master data file containing the assigned unique user passwords shall be limited to the Station or Base ADP System Security Officer (the assigner).

25X1 3) Access to [redacted] data files shall be permitted only at specified and system identifiable terminals, and system output shall be restricted to the same specific identifiable terminals and printers.

c. User Identifiers (Passwords)

25X1 1) User access to an [redacted] data file shall be controlled through the use of a unique identifier (Password), and shall be authenticated by the system each time the user desires to access the data processing system.

2) The password shall not be printed or displayed at any terminal and shall be considered to be at the highest classification level of the data processed by the system insofar as its issuance, individual handling, and storage.

3) User data file passwords shall be changed and new passwords issued:

a) Immediately following any suspected security compromise, or

b) When it is determined that an individual no longer requires access to the system, or

c) Every six months.

NOTE 1:
These requirements do not apply to stand-alone word processing terminals.

NOTE 2:
For some Stations or Bases located in criteria areas, the ISSO may require more frequent password changes.

6. Audit Trails

All automated information processing systems which utilize an Operating System shall provide an audit trail record capability. The audit trail record, as a minimum, shall accurately reflect:

a. All unauthorized attempts to access the information processing system, any application program, or any data file.

b. All authorized system users who attempt to access an unauthorized application program or data file.

c. Any system user who accesses, or attempts to access, an application program. or data file during non-duty hours.

V System Operation

A. System Preparation

1. Approved physical security safeguards as defined in the overseas location's ADP System Security Program and applicable to the information processing system to be used shall be activated.

2. When no cryptographic equipment is included in an ADP installation, the procedures approved by the Director of Security for controlling personnel access to the ADP Facility, and any remote terminals to be used, shall be activated. When cryptographic equipment is included in the ADP installation, the procedures approved by the Director of Communications, and coordinated with the Director of Security, shall be implemented.

3. All telephones located in the ADP Facility shall be physically disconnected using a plug and jack arrangement, or a WECO 270 disconnect, or secured with an approved cryptographic system.

4. The demountable data and program storage media to be used during processing shall be removed from security approved storage, mounted on the appropriate equipment, and the system made ready for processing.

B. <u>Data Processing</u>

1. All system controls shall conform to those required for the protection of the highest classification of the information being processed.

2. Authentication of system user personnel shall be performed by the ADP system.

3. Should an abnormal data processing system operation occur involving any demountable data and/or program storage media (runaway tape or malfunctioning disk pack), the processing operation shall be stopped and the ADP System Security Officer shall be contacted for a determination of the action to be taken.

4. Following any abnormal system operation, the incident shall be logged and the log maintained.

5. Following an abnormal system operation, the ADP System Security Officer shall, within 24 hours of the occurance of the incident, notify Headquarters via ROUTINE cable slugged [redacted] of the incident and the corrective action taken. 25X1

6. Following an abnormal system operation, the System Operating System shall be reloaded and the information processing system reinitialized.

7. Should a security deviation (i.e., a suspected security compromise) occur during the data processing operation, the processing operation shall be stopped, and the ADP System Security Officer contacted

SECRET

immediately for a determination of the action to be taken.

8. Following a suspected security compromise, the incident shall be logged and the log maintained.

25X1

9. Following a suspected security compromise, the ADP System Security Officer shall, within 24 hours of the occurance of the incident, notify Headquarters via PRIORITY cable slugged [redacted], unless the Chief of Station or Base determines that an IMMEDIATE OR IMMEDIATE NIACT cable is indicated by the circumstances of the incident. Corrective action taken by the ADP System Security Officer will be included. If cryptographic material is involved in the incident, an INFO copy of the cable will be provided the Communications Security Division (CSD), Office of Communications by the inclusion of the COMMO slug.

10. Should an act of nature or man-initiated emergency occur (e.g. fire, earthquake, riot, terrorism) or threaten, the ADP System Security Officer shall be contacted immediately. The ADP System Security Officer shall prepare to initiate appropriate emergency procedures. See Section VIII. Actual destruction of any storage media or equipment shall be at the direction of the Chief of Station or Base, or when loss of control of the Facility is imminent.

C. Processing Termination-Normal

1. All demountable data and program storage media used or produced during the processing operation, including the Operating System, shall be removed from the appropriate device.

2. All demountable data and program storage media used during the processing operation, incuding the Operating System, shall be labeled and placed in security approved storage.

3. The automated information processing system Main Power Switch shall be placed in the OFF position.

4. All classified waste, notes, listings, printer and console ribbons for disposal shall be handled in accordance with established procedures for destruction of classified waste.

5. All output such as printouts shall be placed in security approved storage.

6. The ADP Facility shall be secured in accordance with

the procedures approved by the ISSO and defined in the location's ADP System Security Program.

7. All user terminals located in positions remote from the ADP Facility shall be secured in accordance with the procedures approved by the ISSO and defined in the location's ADP System Security Program.

D. Processing Termination-Emergencies

See Section VIII, Emergency Procedures.

VI System Equipment Transportation and Storage

A. Transportation

The transportation of automated information processing system equipment for installation in overseas locations, and the return of system components and equipment for repair/maintenance, shall be accomplished using the currently available TECHREQ procedure.

B. Storage

The Chief of Station or Base shall provide storage for all automated information processing equipment received and waiting installation in an area which meets the security requirements established in Section IV, Paragraph A3a.

VII System Maintenance/Modification

A. System Hardware

1. Maintenance

All on-site maintenance of automated information processing system equipment installed in an overseas location shall be performed by [redacted] personnel assigned to the Area Telecommunications Office, Office of Communications. 25X1

2. Modifications

All on-site changes of equipment configuration, or modifications to an existing system component, shall be:

a. Approved, in writing, by the Chief, Information

Systems Security Group, and

25X1

b. Accomplished by [redacted] personnel assigned to the Area Technical Office, Area Headquarters, Office of Communications.

B. <u>System Software</u>

1. <u>Maintenance/Modifications</u>

a. All automated information processing system software (programming) maintenance and/or modifications shall be accomplished under the control of the Responsible Headquarters component office and provided to the overseas location as a completely tested and operational module or software package.

b. The responsible ISSO shall, in coordination with the Responsible Headquarters component office, review all system software modifications and certify, in writing, that the modification does not impact adversely the security profile of the modified system.

VIII <u>Emergency Procedures</u>

A. In coordination with the ISSO and the Station or Base ADP System Security Officer, the Headquarters component office having primary responsibility shall develop, document, and maintain the following automated information processing system emergency procedures.

1. Emergency Sanitization - Data and Program Storage Media

2. Emergency Protection - Data and Program Storage Media

3. Emergency Protection - Word and Data Processing Equipment

4. Emergency Destruction - Data and Program Storage Media

5. Emergency Destruction - Word and Data Processing Equipment

B. Each Emergency Procedure will be submitted to the Chief, Information Systems Security Group for final approval. The Chief, Information Systems Security Group shall, as appropriate, coordinate each Emergency Procedure with the Overseas Security Support Branch (OSSB), Office of Security, the Communications Security Division (CSD), Office of Communications, and the Technical Security Division (TSD), Office of Security, prior to final approval.

C. Procedures for the handling of cryptographic equipment and materials in emergencies shall be in accordance with the requirements stated in the Station or Base Communications Facility Emergency Destruction Plan and any additional local procedures agreed upon between the location's ADP System Security Officer and the Telecommunications Officer.

ALL PORTIONS OF THIS DOCUMENT ARE SECRET

SECRET