~~SECRET~~ ~~TK/G/H/~~

BIF - 008 B-M-08824-I-80
This document contains 41 pages
Copy ____ of ____ copies
Date 26 March 1980

ADVANCED IMAGE PROCESSING

AND RECORDING LABORATORY

OPERATIONAL SECURITY PLAN

(b)(1)
(b)(3)

WARNING NOTICE

Sensitive Intelligence Sources and Methods Involved

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

DERIVATIVE CL BY: BYE-1
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 12065
REVIEW: 26 March 2000
DERIVED FROM BYE-1

HANDLE VIA BYEMAN /TALENT KEYHOLE
CHANNELS JOINTLY

~~SECRET~~ ~~TK/G/H/~~

TABLE OF CONTENTS

(b)(1)
(b)(3)

1.0 INTRODUCTION, PURPOSE AND OBJECTIVES

1.1 INTRODUCTION

The Advanced Image Processing and Recording Laboratory (AIPRL) has been established at the BIF-008 Bridgehead Facility to support investigations of current and future digital image recordings and to provide a secure computer to process compartmented security information. The major components are an IBM S/370-158 computer (R&E Data Center), an Image Display Station (IDS) and a Laser Writing Device (LWD).

1.2 PURPOSE

This plan describes the security measures currently in effect, and actions which are planned to ensure protection and safeguarding of Sensitive Compartmented Information (SCI) while being processed by Automated Information Systems (AIS). (b)(1) (b)(3)

It likewise provides that, in addition to other security requirements, classified information contained in the ADP system will be safeguarded by the continuous employment of protective features in the system's hardware and software design, and utilizing other administrative, physical, personnel, and communications security controls.

1.3 OBJECTIVES

The objectives of this plan are to establish and detail the methods, procedures, practices, and actions required for multi-level processing of SCI, which at this time, includes information relating to TK and Byeman Programs G, H, [redacted] Where possible, it is the objective of this plan to implement security policies, guidelines and requirements as prescribed by Program B Headquarters. (Reference: Security Requirements for Automated Information Systems). Any deletions or modifications to the plan will be coordinated and reported via the BIFSCO/RSO to the Cognizant Security Office as applicable.

2.0 RESPONSIBILITIES

2.1 ADP SYSTEM SECURITY REPRESENTATIVE

BIF-008 plans to appoint an ADP System Security Representative. The ADP System Security Representative will physically be located at the Bridgehead Facility and report to the BIFSCO. This individual will be available and respond to the Bridgehead Program Manager and the AIPRL Operations Manager in providing professional security guidance.

The BIF-008 ADP System Security Representative will be charged with, at least, the following responsibilities:

a. Implement and ensure compliance with security portions of this document.

b. Develop, implement, and maintain ADP security plans that relate to AIPRL activities. (b)(1) (b)(3)

c. Serve as liaison between BIF-008 and Customer on the subjects of ADP security, RFI emanations, and Tempest requirements.

d. Establish and maintain security programs for word processing systems, micro-, mini-, and computer systems including computer microforms, and support equipment.

e. Review all electrical hardware planned for use to process SCI material to ensure security compliance, RFI emanations and Tempest conditions, etc.

2.2 PROGRAM MANAGER

The Program Manager is responsible for the operation of the Bridgehead Facility. This includes directing the effective use of customer furnished equipment and proper safeguarding of customer information necessary for the operations and research efforts carried out in fulfillment of contracts.

2.3 AIPRL OPERATIONS MANAGER

The AIPRL Operations Manager provides overall direction for R&E Data Center operations. He approves procedures, installation of new software products, and non-vendor supplied patches; maintains records of all software product revision levels and patches installed; determines scheduling priorities; and reviews routine accounting and security reports for suspicious activity.

2.4 CHIEF SYSTEMS PROGRAMMER

The Chief Systems Programmer oversees the system generation and maintenance; advises the AIPRL operations manager of operating system revision, and patches; and provides troubleshooting support when operational problems are encountered.

2.5 COMPUTER OPERATORS

Computer operators have security responsibilities to handle classified materials within the computer room; ensure that classified materials are properly secured at shutdown; and investigate attempts to thwart system safeguards, e.g. - repeated use of invalid password.

2.6 INPUT/OUTPUT CLERK

The Input/Output Clerk also handles classified materials within the computer room and assists operator in securing classified materials at shutdown. With operators, he issues special group tapes to users, and maintains accountability logs for these tapes. He maintains a log of batch jobs and tapes entering or leaving the computer room.

3.0 FACILITY DESCRIPTION

3.1 GENERAL DESCRIPTION

The AIPRL Computer occupies the ground floor of Building 2 at the Bridgehead Facility. This four-story building is part of a 7-building complex. The AIPRL area is surrounded by a TEMPEST RF shield, which is made up of 3/4-inch thick particle board with 20-gauge galvanized steel bonded to each side. The joints are bolted at 3-inch intervals. The interior contains raised flooring and suspended ceilings throughout. The interior is divided into rooms by steel "Hausermann" partitions with under-floor and over-ceiling extensions. (See Figure 3-1)

Access will normally be through the automatic door at 26. There are manual doors in the RF shield at either end which may be used for fire exits or for moving equipment. As opening these doors violates the TEMPEST RF shield, all sensitive data processing must be secured while these doors are open.

3.2 SECURITY SAFEGUARDS

3.2.1 Physical

3.2.1.1 Facility

The AIPRL area is located at BIF-008 B's Hawk-Eye Plant, which is situated at the corner of St. Paul Street and Driving Park in Rochester, New York. Figures 3-2 through 3-6 show floor plans for those buildings at Hawk-Eye Plant that contain BIF-008 B's Bridgehead areas.

Byeman areas are outlined with heavy dark lines. They are located in Buildings 1, 2, 3, 6, 9, 10, 11, 12 and 13 which are located at the north end of the Plant. The AIPRL processing facility is located on the ground level of Building 2. The General Configuration is shown in Figure 3-1 and the detailed floor plan of the computer room is illustrated in Figure 3-7.

The Hawk-Eye Plant is a BIF-008 owned facility. As a minimum, the following company security services are provided:

a. A completely fenced perimeter length (8) foot chain link barbed-wire topped.

b. Uniformed guards at open entrances.

c. Inspection of incoming/outgoing packages.

d. A picture pass system for entry to the plant.

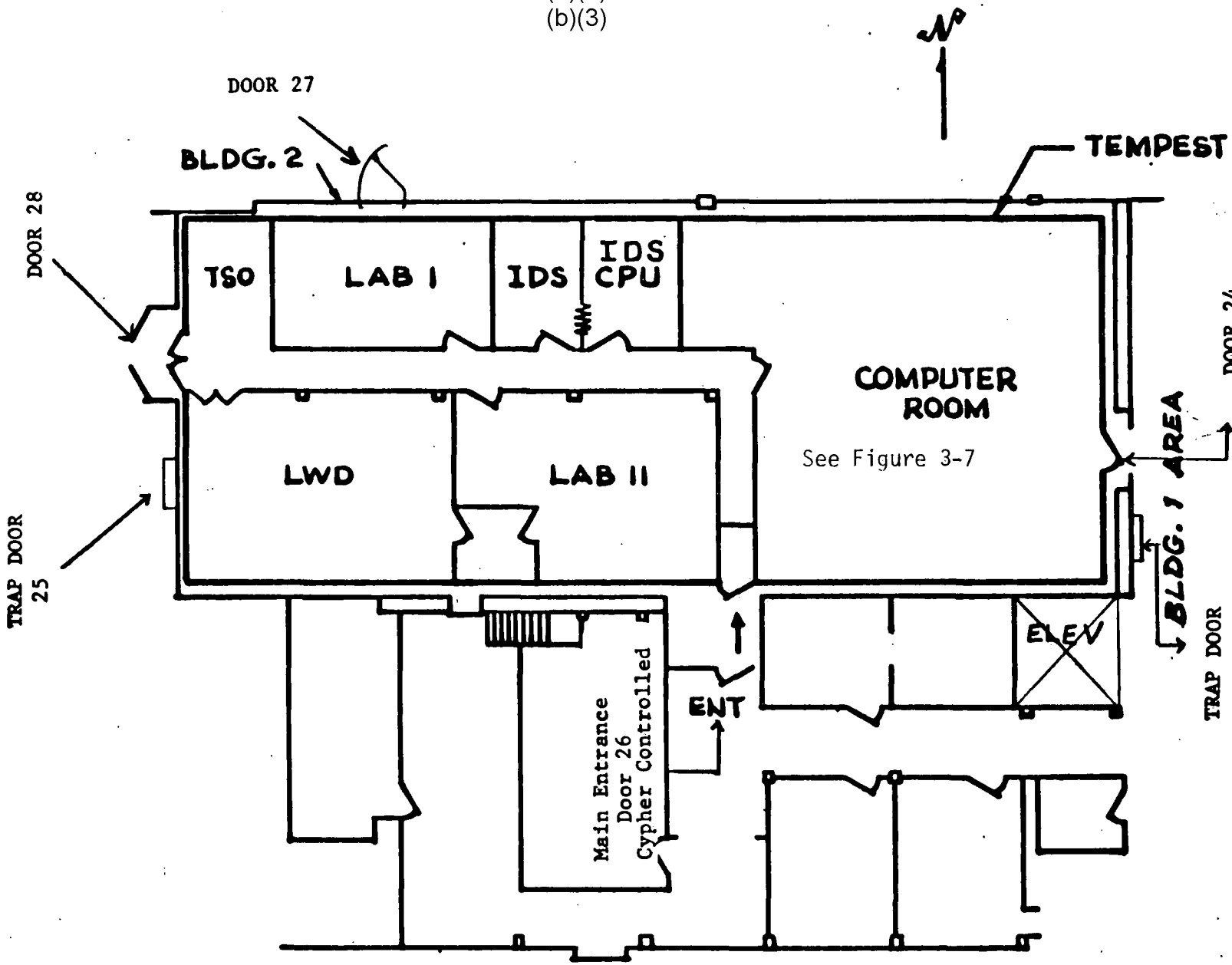

Figure 3-1, AIPRL Floor Plan

HANDLE VIA BYEMAN/TALENT KEYHOLE CHANNELS JOINTLY

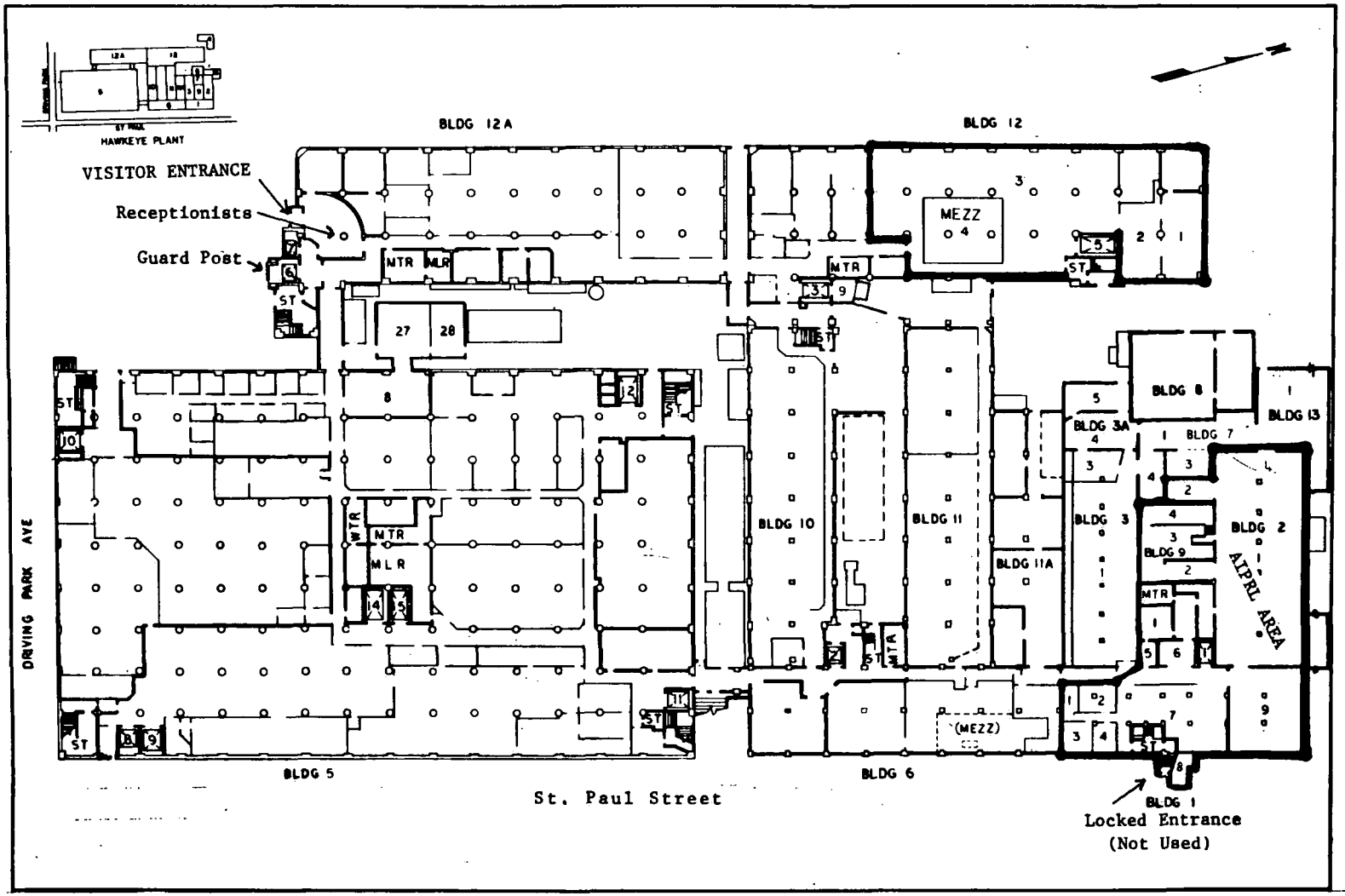

Figure 3-2, First Floor Plan

(b)(1)
(b)(3)

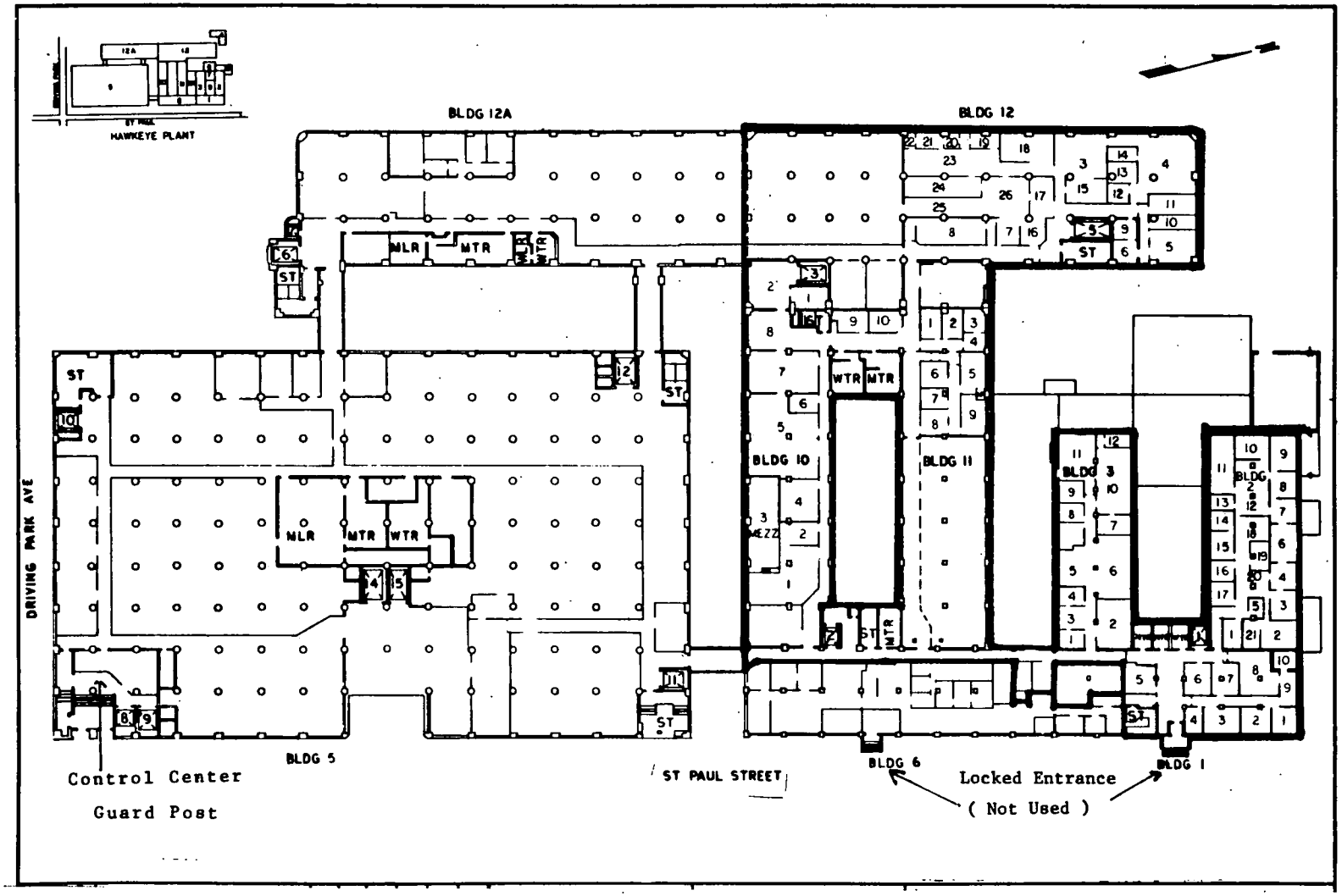

Figure 3-3, Second Floor Plan

(b)(1)
(b)(3)

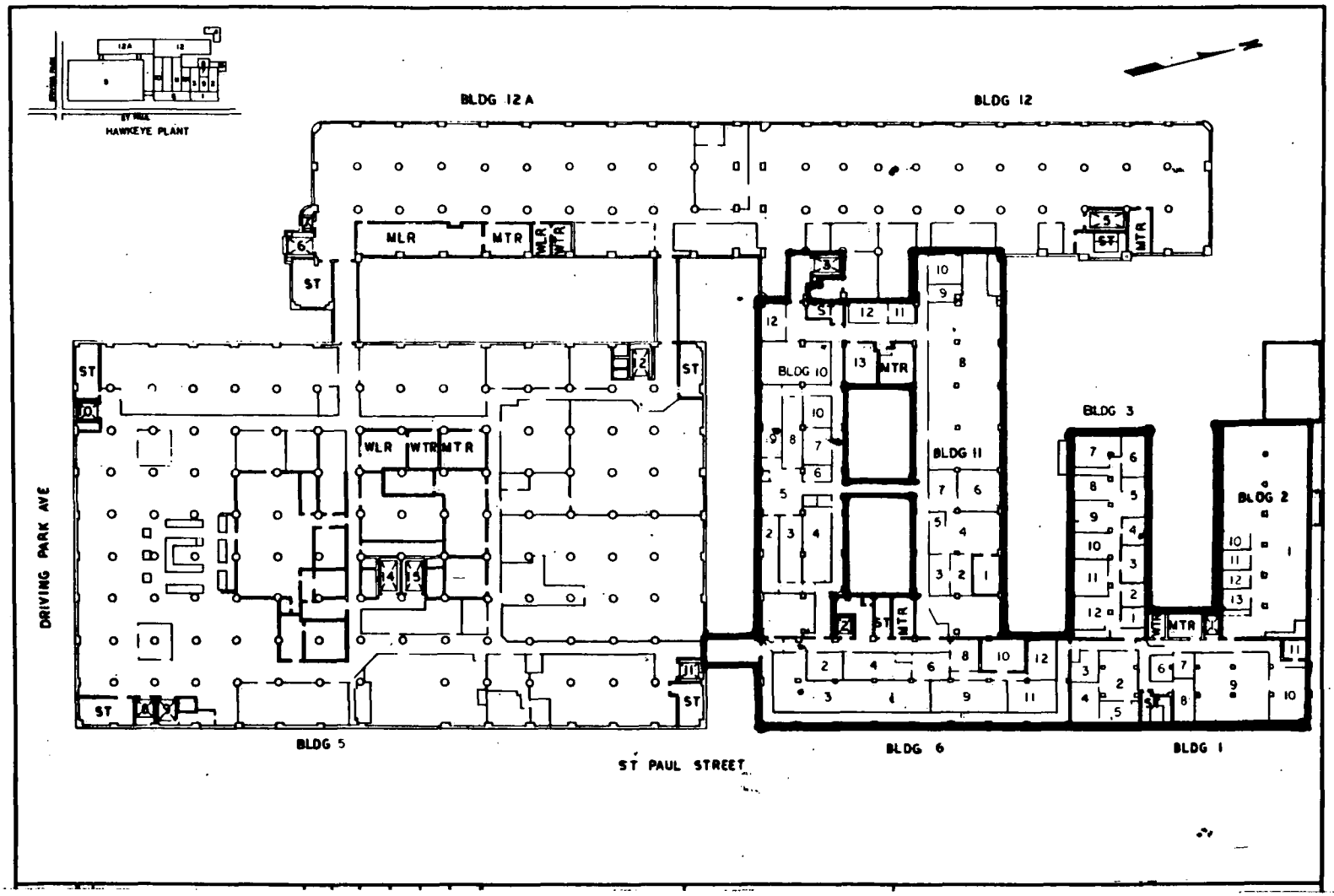

Figure 3-4, Third Floor Plan

(b)(1)
(b)(3)

~~SECRET~~ TK/G/H

~~SECRET~~ TK/G/H

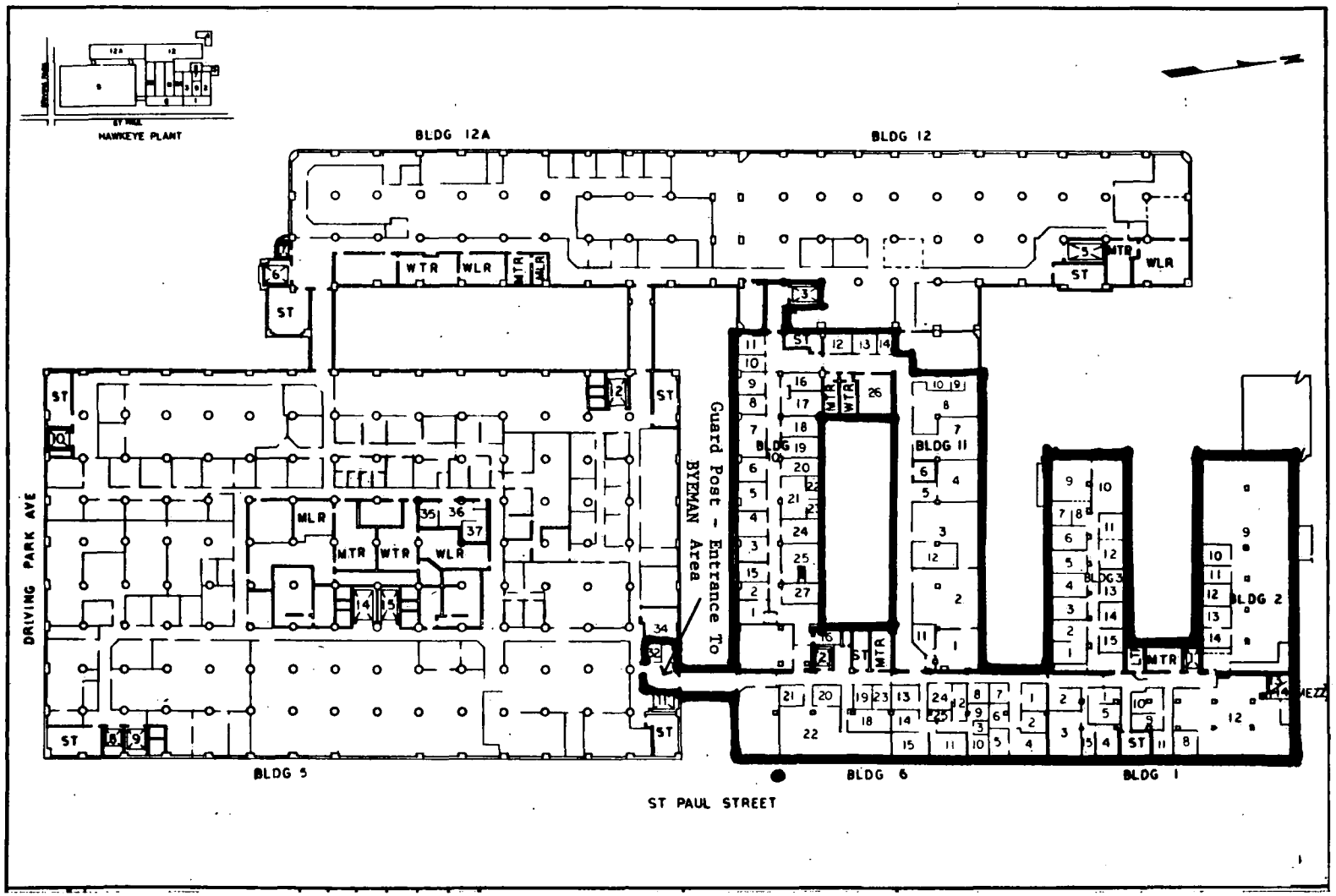

Figure 3-5, Fourth Floor Plan

(b)(1)
(b)(3)

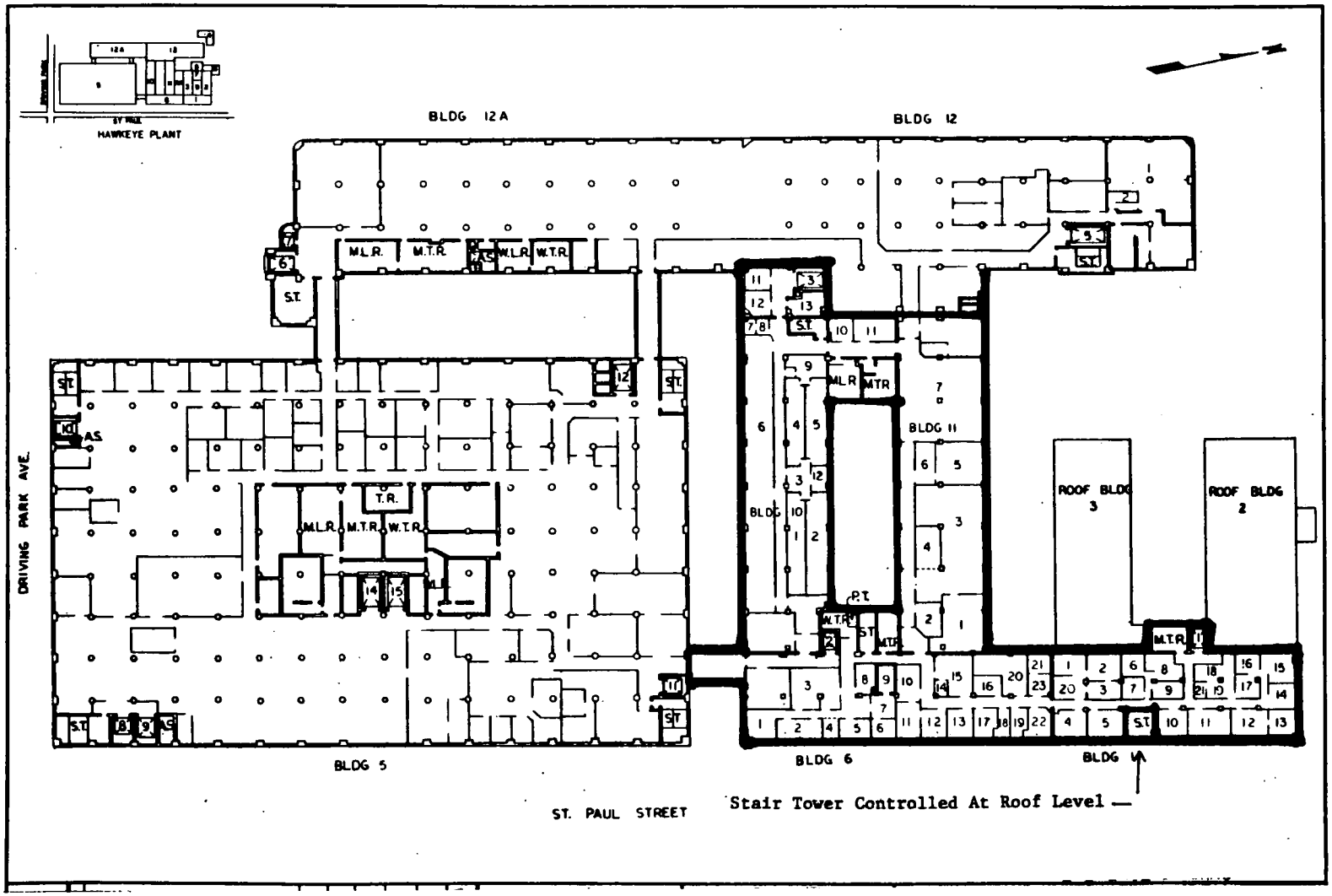

Figure 3-6, Fifth Floor Plan

(b)(1)
(b)(3)

~~SECRET~~ TK/G/H

~~SECRET~~ TK/G/H

(b)(1)
(b)(3)

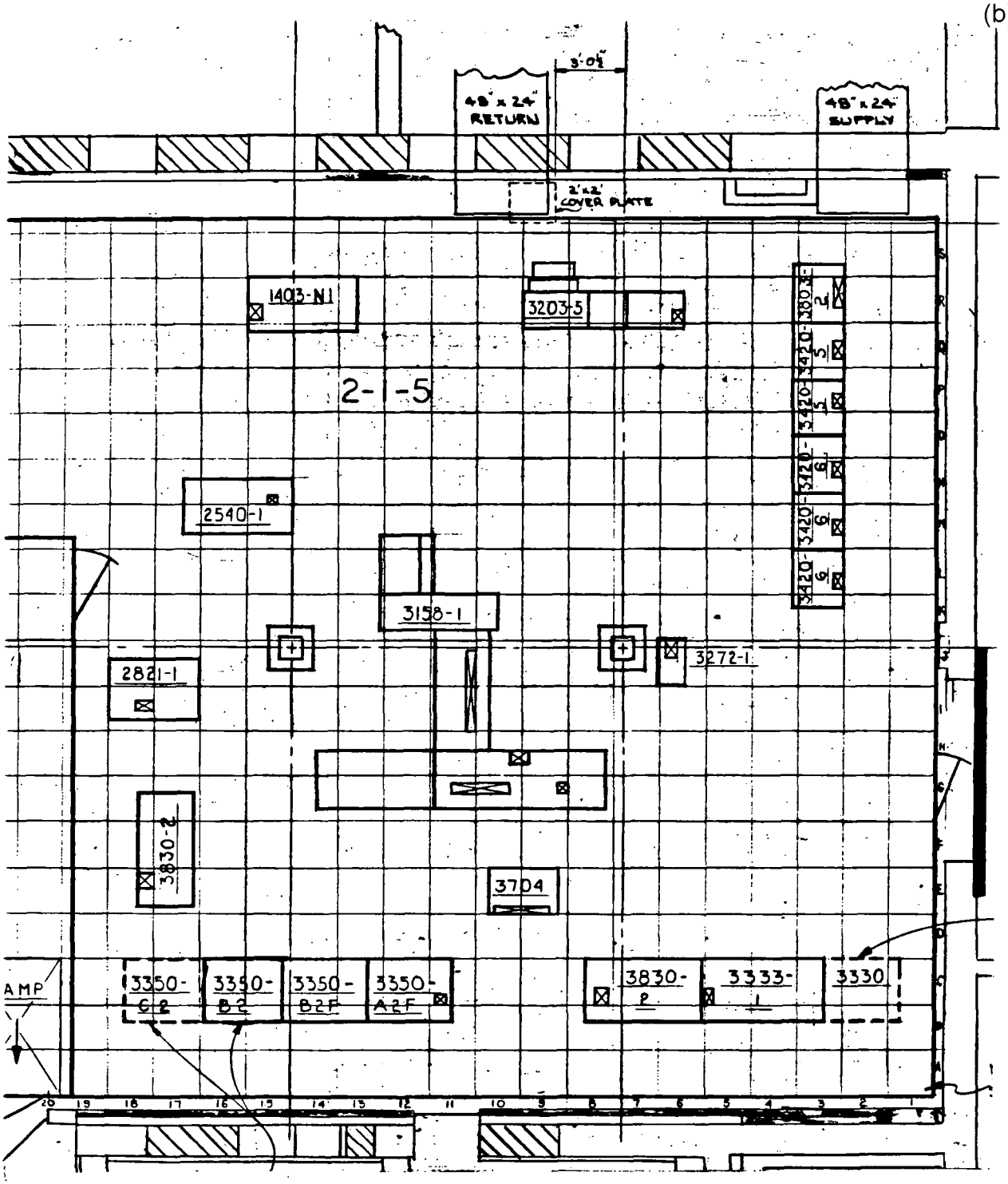

Figure 3-7, Computer Room Equipment Layout

HANDLE VIA BYEMAN/TALENT KEYHOLE
CHANNELS JOINTLY

~~SECRET~~ ~~TK/G/H/~~

3.2.1.1 (continued)
In addition, BIF-008 has a thorough and detailed plan for dealing with emergencies. BIF-008 general management personnel, who are Byeman briefed, actively participate in the preparation of such plans and therefore not only have the company's commercial interest in mind, but Byeman commitments as well.

The Hawk-Eye Plant has personnel entrances at only three points: One on the first floor of Building 12A and two on the second floor of Building 5. The entrance at the southeast corner of Building 5 (Figure 3-3) is the main guard control station and is continuously manned. The entrance at the northeast corner of Building 5 (Figure 3-3) is open from 6:30 A.M. to 5:30 P.M. on normal workdays and is manned by a guard. Dock areas, when open, are manned by uniformed Security Guards.

3.2.1.2 PERIMETER CONTROL (b)(1) (b)(3)

Figure 3-1 reflects a detailed layout of the AIPRL Facility, which encompasses the entire first floor level of Building 2. Building 2 is a brick and mortar structure with poured reinforced concrete floors.

There are no windows and the one door, north wall (#27), which leads to the outside of the building is locked, alarmed and secured with an S&G combination padlock Model Number 8077A. Access to the AIPRL area will be by use of elevator number 1, which is located adjacent to Building 2, or by the stairwell. Both the elevator and stairwell have access only within the Byeman perimeter.

The AIPRL area is within a TEMPEST enclosure, located within the overall Byeman perimeter and compartmented from other Byeman activities in the total facility. Entrance to the AIPRL facility, door 26, is controlled by a Rusco Electronics R15R-ID Electronic Cypher unit. For downtime purposes, the entrance door will be secured with a S&G safemaster, extension 50 locking device. The door is equipped with a magnetic contact door action which will be activated, during downtime, as part of the security of the area procedure.

Doors 25 and 25A are trap doors which allow access to the overhead of the TEMPEST enclosure. These doors are alarmed, locked and sealed. These doors will be used to afford access to inspect the enclosure as required and allow program approved maintenance and facility personnel to inspect sprinkler systems, air conditioning equipment etc. Doors are locked, sealed and alarmed to the Wells Fargo annunciator panel located at the 24-hour guard post. Doors 28 and 29 are emergency exits and equipment access doors which are sealed and alarmed on the Wells Fargo Annunciator.

3.2.1.3 Security

Uniformed, unarmed guards provide plant-wide physical protection of buildings, and grounds, internal patrolling, guarding and escorting and monitoring of alarm systems. In addition, BIF-008 Plant Security provides company identification badges and conducts investigations of any suspected or actual criminal, subversive, or civil disorders on plant property. All Security Officers carry communciation equipment so that they can be contacted in the event of an emergency situation or when help may be requested by another security officer. All guards assigned to the Bridgehead Byeman area have been Byeman approved and briefed. Security Officers are BIF-008 employees.

3.2.1.4 Locking Mechanism

Locking devices used in the AIPRL Facility will include:

(b)(1)
(b)(3)

a. S&G Safemaster, Extension 50.

b. S&G Combination locks, Model 8D77A.

c. Rusco Electronics card/cypher unit model: R15R-ID.

3.2.1.5 Alarm System

The alarm system for the facility consist of two operating systems:

a. One volumetric alarm system: Advisor VIII High Security Ultrasonic Matron Detective System, 2 Zone Installation. One zone covers the computer room and the other covers the remainder of the AIPRL area.

b. The Firetek Pre-action Sprinkler system covered in Section 3.2.3. Both systems are electronically connected to the Wells Fargo Annunciator System located at the 24-hour guard post.

3.2.2 Emanation Control

3.2.2.1 TEMPEST

The AIPRL computer and peripherals are completely located within a TEMPEST enclosure which was tested to MIL-STD-285 and NSA 65-6 on

3.2.2.1 (continued)
26 March 1980. The enclosure is equipped with an automatic door at the main entrance, and a fire exit/equipment door at either end. In addition to the filtered penetrations for power, telephones, alarms, etc., there is a 4-inch diameter wall port in the computer room. The opening of either fire door or the wall port VIOLATES the TEMPEST integrity, and no classified data my be processed at this time.

3.2.2.2 Data Link

It is anticipated that at some time in the future, a secure communications link will be established to support remote job entry (RJE) from Building 101, approximately 10 miles away. Components of this link will include the IBM 3704 communications adapter, filtered penetrations of the TEMPEST enclosure, and shielded or fiber-optic lines to the multiplexer/encryption unit. (b)(1) (b)(3)

At Building 101, there will be a commercially available RJE station and a customer furnished encryption unit in a COMSEC approved environment. RJE operators will have adequate clearance and procedures to handle any accidental data spillover which might occur.

3.2.3 Fire Protection

The AIPRL facility is protected by a FIRETEK Pre-Action Sprinkler Sytem. This is a normally dry system which has several safeguards against accidental discharge and yet will provide extinguishment in the quantity needed.

The Pre-Action system is composed of a sprinkler piping with normal sprinkler heads having fusible links; a heat detector next to each sprinkler head set to 135°F, a lower temperature than the fusible link melting temperature (165°F); smoke detectors; solenoid water valves and back-up power. Additional detectors are located under the raised floor.

Piping to each sprinkler head is normally filled with air at 3 psi in a supervised system. Should there be an air leak or should the fusible link be broken accidentally as with a broom handle, a trouble alarm will sound, but no water will flow. The trouble alarm appears at the 24-hour guard post. Next to each sprinkler head is a heat detector. Should the temperature rise high enough to trip the heat detector, the system is charged with water, but no sprinkler

3.2.3 (continued)
flow will occur until the temperature rises further and melts the fusible link on one or more heads. At the time the heat detector operates, a fire alarm is sent to the Hawk-Eye Main Control Center, and in addition a distinctive local alarm sounds. Simultaneously, the computer power and air conditioning are automatically shut down.

A network of smoke detectors is also part of this system and will probably give the earliest warning; a local alarm bell and an alarm at the 24-hour guard post. The water system is not dependent upon the smoke detector operation.

3.2.4 Personnel

Personnel requiring access to the AIPRL area will have undergone an Extended Background Investigation (EBI), as required by DCID No. 1/14. Physical access to the AIPRL area will be governed by the "need-to-know principle." Each person authorized access, will be approved and briefed on TK and individual Byeman program(s) as appropriate.

4.0 ADP SYSTEM DESCRIPTION

4.1 GENERAL

The AIPRL Computer System is an IBM S/370, Model 158-1, with 5 megabytes of memory. Through the use of a multi-user, virtual storage operating system, IBM OS/VS2, a variety of user jobs may be processed concurrently. The most sensitive are those which perform image manipulation and enhancement on pixel data from TK systems. Another large group of runs will be structural analysis applications using the MSC/NASTRAN software packages and data which may describe classified hardware. Eventually, this NASTRAN data may be entered via a remote-job entry terminal and encrypted data link from Building 101. On occasion, there will be program-specific jobs which support Bridgehead operations. In addition, there will be numerous jobs of short duration to support a variety of engineering analysis and data reduction as a part of ongoing research efforts. These jobs may be typified as prototype software to perform "quick and dirty" tasks, and are not well documented.

(b)(1)
(b)(3)

4.2 R&E DATA CENTER HARDWARE

The following devices comprise the R&E Data Center hardware complement.

DEVICE	UNIT	SERIAL NO.	
CPU	3158	24132	
Storage Control	3830	46558	
Storage Control	3830	46557	
Disk Storage & Control	3333	41077	
Disk Storage	3350 FH	30128	
Disk Storage	3350 FH	59490	
Disk Storage	3350	70120	
Tape Controller	3803	20736	(b)(1) (b)(3)
Tape Drive	3420-6	51T0247	
Tape Drive	3420-6	51T0246	
Tape Drive	3420-6	51T0310	
Tape Drive	3420-5 DD	5159700	
Tape Drive	3420-5 DD	5159057	
Controller	2821	18192	
Printer	1403	33015	
Reader/Punch	2540	10932	
Printer	3203-5	15683	
Controller	3274-1B	24326	
Printer	3289	14345	
Communciation Control	3704	30712	
CALCOMP Plotter	1039	2677	
Plotter Controller	921	2241	

HANDLE VIA BYEMAN/TALENT KEYHOLE CHANNELS JOINTLY

4.2 (continued)
Figure 4-1 shows the functional relationships of these equipments. The physical location of equipment items in the computer room is shown in Figure 3-7.

The S/370-158 mainframe includes the following security-relevant features:

a. Volatile main memory which does not retain data after power shutdown.

b. A memory bounds mechanism so that memory allocated to any particular system user can be restricted to prohibit the user from reading or writing in memory occupied by the operating system, and from writing in memory occupied by other system users. (b)(1) (b)(3)

c. One class of machine instructions reserved for exclusive use of the operating system and one class useable by both the operating system and the user's application programs.

d. A time-of-day clock to provide for the time recording of all events and output.

e. A hard copy output device which can be used for system activity logging (console log).

f. Removable diskette which is required for system startup (IPL).

4.3 SOFTWARE PACKAGES

The initial complement of software includes the following:

IBM Products:

OS/VS2

Fortran H Extended Compiler	5734-F03
Fortran Library Mod II	5734-LM3
Fortran Interactive Debug	5734-F05
Fortran IV G1 Compiler	5734-F02

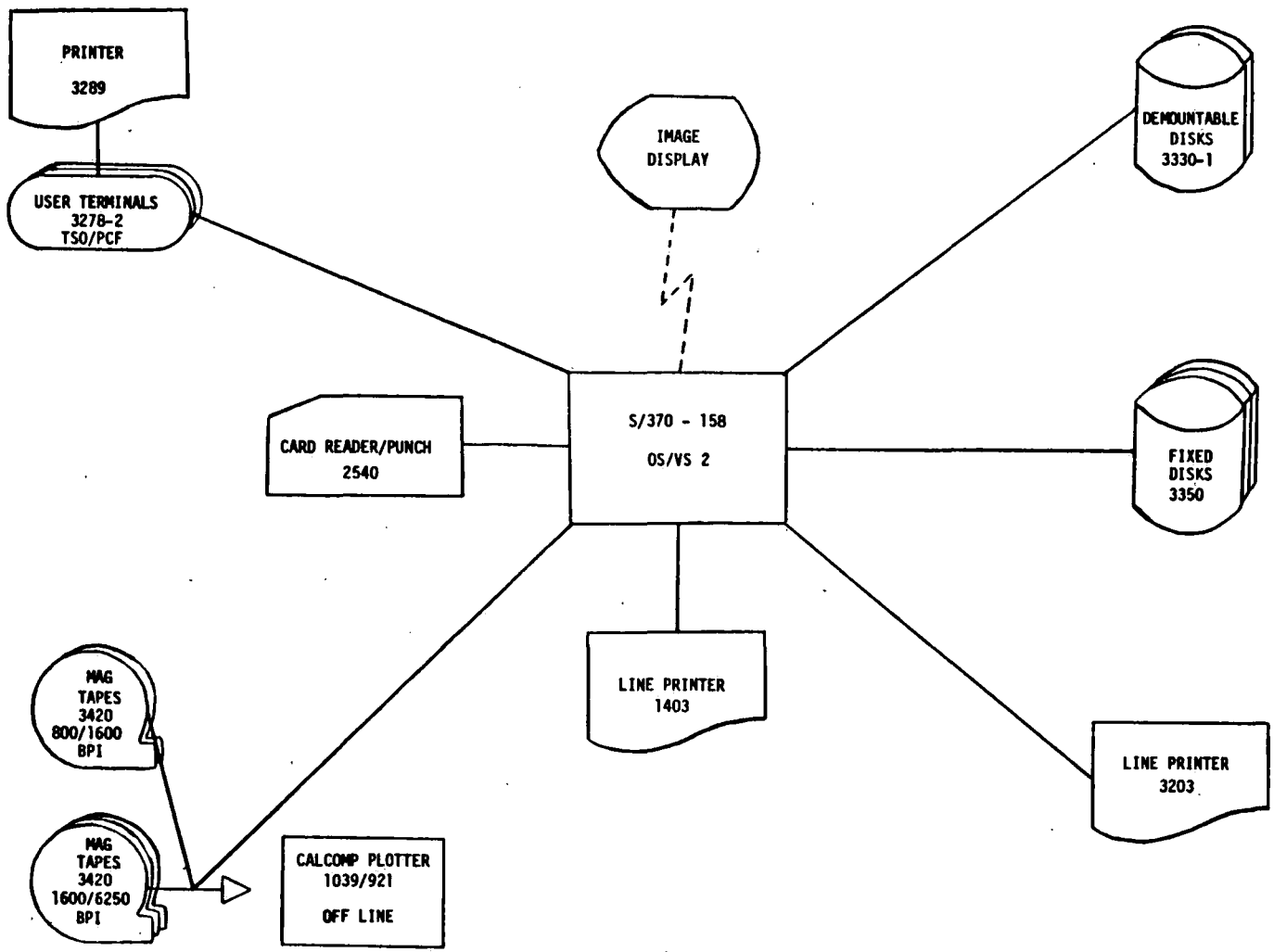

Figure 4-1, AIPRL Computer Functional Configuration

(b)(1)
(b)(3)

4.3 (continued)

Fortran H Extended Optimizer Enh.	5796-PKR
PL/1 Optimizing Compiler and Library	5734-PL3
TSO Command Package	5740-XT6
TSO 3270 Display/SPF	5740-XT8
TSO Fortran Prompter	5734-CP3
TSO Program Control Facility II	5798-CLW
TSO Comman Proc/DSPRINT	5798-AYF
Subroutine Library-Math (Fortran)	5736-XM7
Document Composition Facility W/FG	5748-XX9
Resource Measurement Facility V2	5740-XY4 (b)(1) (b)(3)
General Purpose Simulator System V	5734-XS2
3704 Emulation Program	5744-AN1

Non-IBM Products:

Calcomp Plotter Package	California Computer Products
Syncsort - Sort/Merge	Whitlow Computer Systems
Nastran - Structural Analysis	MacNeal-Schwendler Corp.
Panvalet w/TSO - Source File Management	Panosophic Systems
DYL-250 - File Manipulation	Dylakor Computer Systems
FDR/SDF - Fast Dump/Restore	Innovation Data Processing
SPSS - Statistical Package	SPSS Inc.
PPE - Program Problem Evaluator	Boole & Babbage

4.3 (continued)
Other commercially available or customer-furnished software packages may be added in the future.

In addition to vendor-supplied software, many locally developed programs will be run. These include: System support programs such as the billing/management usage summary programs, the security screening program, and clear disk program.

User written programs such as SCAT3, FASTERK and RENUMBER. Many of these programs are of limited use and are not extensively documented.

The OS/VS2 Operating System provides the following exclusive services:

a. Cause all applications programs to load as scheduled.

b. Allocate memory, direct access storage space, and devices to applications programs.

c. Handle all input/output functions related to available and shared resouces. (b)(1) (b)(3)

d. Handle all interrupts designated for applications programs.

e. Protect itself.

f. Provide an audit trail record (SMF Data). See Audit Trail, Section 7.0.

5.0 SECURITY PROCEDURES

5.1 PHYSICAL SECURITY

Physical protection will be maintained in accordance with requirements of the Byeman Industrial Security Manual, and where applicable, USIB Physical Security Standards for sensitive compartmented information (SCI) facilities.

5.1.1 Access Control

5.1.1.1 Badge System

Color-coded badges are used to control access to Bridgehead program areas: red badges are used for company personnel and green badges are used for non-company personnel. Badges included the individual's name, with coded project accesses and levels. Authority to issue these badges must be in writing from the facility Security Officer. These badges are maintained and controlled at the 24-hour guard post located at the perimeter entrance. Individuals exchange company picture passes for color coded area badges when entering the Byeman perimeter and reverse the procedure when departing. Thus the guard can determine at any time whether an individual is in the area. (b)(1) (b)(3)

Visitors must be certified to BIF-008B, prior to each visit. After certification has been received, a badge is prepared for each visitor showing his certified approvals, name, and date(s) of visit. After the visitor leaves, his badge will be removed from the badge system.

5.1.1.2 Access to AIPRL Facility

Access to the AIPRL facility will be via an electrically operated cypher unit, installed at the main entrance door. Two approved/briefed people will be working in the AIPRL facility at all times when classified data is being processed.

5.1.1.3 Facility Maintenance Personnel

BIF-008B facility maintenance personnel are Byeman approved/briefed and will be granted access to the area as appropriate.

5.1.1.4 System Services Personnel

Several Customer Engineers from BIF-191 will have been approved for access to the Facility and will provide service to the equipment as required.

Personnel who are not approved for program access, such as fire and safety inspectors, other maintenance and equipment service personnel, will be admitted under escort.

5.1.2 Storage

5.1.2.1 GSA Containers

Storage in the AIPRL area will be by GSA approved storage container and computer media cabinet specially equipped with hardware for securing with S&G combination locks model 8077A.

(b)(1)
5.1.2.2 Non-Removable Disks (3350) (b)(3)

Generally these disks will not have classified data written on them; however, these cabinets will be modified with external locking devices. These disks, like the rest of the area, are protected by a volumetric alarm system.

5.1.3 Transportation

5.1.3.1 Intra-Facility

Within the program areas, approved personnel may carry sensitive material from one work area to another. Materials will be under cover to preclude unauthorized sight access.

5.1.3.2 Inter-Facility

A Byeman messenger service is used to transmit sensitive materials between plants. Two approved people will make deliveries four times daily between BIF-008's locations in the metropolitan area.

Each package containing classified materials will have a formal transmittal receipt attached to it to transfer and maintain appropriate accountability from the messenger to the addressee in the other facility.

5.1.4 Facility Opening

At the start of the work day, Monday through Friday, an approved Security Officer will unlock door 26 main entrance to the AIPRL facility. The first person to enter the area Lab or Computer Room will inform the Security Officer at the Guard Post by telephone that they are entering the area and will deactivate the alarm system for the Lab areas and for the Computer Room. The Security Officer at the Post will then place the alarm drop in the day mode for clear access, and make the appropriate entries in the guard log.

Downtime Admittance

After-hour admittance is handled in a number of ways - if a regular work schedule was arranged, the guards are so notified and those scheduled are admitted to the area. If the work is not scheduled an overtime (access) authorization is furnished to the guards and admittance for overtime is authorized. Visitors, on occasion, by prearrangement, are escort-admitted into the area. In this case visitor authorized badges are furnished to the guards and the escort is so identified and the date and time are stipulated.

5.1.5 Facility Closing (b)(1) (b)(3)

5.1.5.1 Computer Room

Execute flush procedure.

Execute system end-of-day procedure.

Demount any tapes and removable disks.

Turn off disk drives, tape drives, controller, printers, and plotter.

Dim console and remove key, remove diskette.

Secure any unclaimed jobs.

Secure tape and disk cabinets.

Lock I/O counter doors.

Seal lock up burner boxes.

Call Security Officer who will check cabinet locks and activate alarms.

HANDLE VIA BYEMAN/TALENT KEYHOLE CHANNELS JOINTLY

5.1.5.2 Facility

The last person to leave the facility will call a security officer who will check all lab doors, conduct an investigation of the AIPRL Facility, activate alarms and secure door #26.

5.1.6 Data and Program Storage Media

5.1.6.1 Removable Disks (3330)

All 3330 Disks except specially marked "SYSTEMS PROGRAMMER USE ONLY - NON SENSITIVE", shall be considered to have once contained sensitive customer data. These disks will be stored overnight in bar locked cabinets within the computer room.

Vendor Supplied Floppy Disks - These diskettes contain microcode and diagnostic software for the computer mainframe and some controllers. They are unclassified and are normally stored in the equipment itself. They will retain the vendor's markings. At shutdown, the CPU Diskettes will be placed in a locked cabinet. (b)(1) (b)(3)

5.1.6.2 Non-Removable Disks (3350)

Users will not generally write classified data onto the 3350 disk units. However, the operating system may at times write such data onto temprorary data sets, page data sets, spooling files, etc., so they must be considered sensitive.

The cabinets for these drives shall be fitted with external locking bars to make unauthorized disassembly and removal of magentic storage media more difficult. These disk drives, like the rest of the computer room, are protected with intrusion alarms, and the facility perimeter doors are equipped with contact alarms.

5.1.6.3 Punched Cards

Cards may have classification markings clearly written or stamped on them and if so, will be handled accordingly. All user submitted jobs with program or data cards will be treated as "sensitive" e.g., logged in, secured if left overnight, etc. Similarly all cards punched by user jobs shall be treated as "sensitive" while in the computer room.

5.1.6.4 Magnetic Tapes

There will be several categories of magnetic tapes. Once assigned to a category the tape will be marked, with a distinctive color code, given an appropriate ID, and will not be designated for a less sensitive use. The categories are:

a. User unclassified tapes, e.g., AB, BB, or UU. These tapes will normally be submitted by users and may be returned with the completed job. These tapes will be handled as UNCLASS while in the computer room, but stored in a locked cabinet if left overnight.

b. User classified tapes, e.g., HH or CC. These tapes will be submitted by users with a transmittal receipt form, and maybe returned with the completed job. A signature will be required for removal from the computer room. (b)(1) (b)(3)

c. System support tapes, e.g., SS. These tapes will be used for backup of disk data sets, retention of SMF data, backup of PANVALET libraries, etc. These tapes will always be retained within the computer room or designated locked safe/vault. The I/O clerk or operators will maintain a log of such tapes and their whereabouts.

d. Commo Tapes (XX): These tapes contain message data either incoming or outgoing. They will normally not be retained in the computer room, but may occasionally remain overnight, in a locked file. The prefix XX will be added to the identification assigned by the communications group to form an unclassified tape ID. Classified "slugs" will NOT be used in the tape ID.

e. Image Tapes (KK): A large group of tapes will be reserved for pixel data from operational (TK) imagery or enhanced version thereof. These tapes may circulate to the LWD or IDS, but will be stored overnight in bar locked tape cabinets within the computer room, or within a safe/vault. Each tape will be assigned a rack position and a log will be maintained nearby to record user, and whereabouts if out.

(Continued)

f. Vendor supplied diagnostic and program product tapes. These are unclassified tapes that should not be written on. They will retain the vendor's markings. They will normally be stored in a locked cabinet when not in use.

STORAGE MEDIA CODES

	Prefix	Color
Commo Tapes	XX	Red
Image Tapes	KK	Orange
System Support Tapes	SS	Blue

(b)(1)
(b)(3)

5.1.7 Printed Output Storage

The user may, under program control, print a security classification at the top and bottom of each page. Other printed output, though usually not sensitive, will be treated as such. To minimize risk of data spillover, jobs left overnight will be secured in GSA approved locked containers.

5.1.8 Accountability

5.1.8.1 Logging

All batch jobs and tapes will be logged in and out of the computer room by the I/O clerk or an operator. Jobs being returned to other locations will be logged separately and placed directly in a pouch for Byeman messenger.

Tapes stored in the computer room will be arranged by category and ID number with a rack position for each tape. The I/O clerk and/or operator will maintain a log near each rack showing the use assigned to each tape, the user, and whereabouts if removed from the computer room.

5.1.8.2 Destruction

Waste paper and cards will be placed directly in classified burner containers and disposed of following customer-approved procedures.

5.2 DATA AND PROGRAM SECURITY

5.2.1 Access Controls

5.2.1.1 System

To prevent unauthorized use of the computer during shutdown, the mainframe operational diskette and console key will be removed. In addition, should the system be powered down for an extended period, a combination lock will be placed on the power panel.

5.2.1.2 Terminals/Data Files

An authorized user may initiate a TSO session by entering the AIPRL facility and logging on a terminal. LOGON will require entering a 3-8 character non-echoed password, which must correspond to the user's ID number. Successful LOGON will grant the user access to the PANVALET library and program data set(s) assigned to his group. (b)(1) (b)(3)

Access to a specific PANVALET file may be further limited through use of the ++ ACCESS command.

Access to protected data sets and restricted libraries (Assembler, certain utility programs, etc.,) will require additional OS data set passwords of 3-8 characters. Non-temporary storage of classified data will be on removable media, e.g., tape or 3330 disk pack.

5.2.2 Passwords

5.2.2.1 Issuing/Changing

The 3-8 character passwords are like safe combinations, and will be treated as such. Any list of passwords will not include user ID number.

The password will be issued by the ADP Security Officer, who will maintain indirect referenced lists of all passwords. The ADP Security Officer may designate specific Data Management programmers to update and maintain the system password file in a protected data set.

(Continued)
Individual passwords will be changed when users leave or have no further need to use the computer. All passwords will be changed when compromise is suspected or upon the departure of the ADP Security Officer, a designated data management programmer, the chief systems programmer, or principal customer engineer. Otherwise passwords will be changed on the same schedule as provided for safe combinations.

5.2.3 Sanitization

5.2.3.1 Magnetic Tapes

A magnetic tape, once assigned to a sensitive use, will be used in that capacity until no longer serviceable, at which time all or part of it will be destroyed by burning. If it becomes necessary to sanitize such a tape, it will be done on a customer approved degausser such as the Bell & Howell TD-2903-4B, following the manufacturer's directions. The degausser cycle will be repeated 3 times. All classification markings and/or color codes will be removed. The ADP Security Officer will ensure that the degausser is properly maintained and periodically inspected to ensure its continuing effectiveness. (b)(1) (b)(3)

5.2.3.2 Disk Packs

Disk packs if operable, will be sanitized by setting all data locations to zeros, verifying the pattern, rewriting all data locations to ones, and verification repeated. This cycle shall be repeated at least 3 times.

If damaged or inoperable, they will be disassembled and the magnetic media physically destroyed by customer approved means.

5.2.3.3 Non-Demountable Disks (IBM 3350)

In the event of decommissioning or non-repairable failure, the 3350 disk head assemblies (HDA's) will be removed, and physically shipped by customer approved means to a secure area at IBM, Gaithersburg, MD, for disassembly. The magnetic recording surfaces will then be transported by customer approved means to a designated customer facility for destruction.

5.2.3.4 Main Memory

The S/370-158 CPU has MOSFET memory, which will not retain data after power is removed. The memory shall be considered unclassified after it has been powered down for 5 minutes.

5.2.4 Software Modifications

Routine modifications to the operating system which are supplied by the vendor will be implemented by the chief system programmer. Locally derived patches, if any, will also be approved by the AIPRL manager. The AIPRL operation manager, or his delegate, will maintain a record of all vendor program revision levels and patches/fixes installed.

User-written software will be controlled by the user, and may be modified at will.

5.3 SECURITY VIOLATIONS (b)(1) (b)(3)

5.3.1 Physical

Any breach of physical security will be reported to the RSO, (Resident Security Officer, Program B) and to the appropriate program office upon completion of an intensive investigation. Violations include such items as security container left open, unauthorized door openings, classified material left out and compromise of passwords.

5.3.2 Data

An inadvertent spillage of data to terminals users will be investigated immediately. The suspected compromise will be brought to the RSO's attention and, if necessary, the individual will be given a defensive briefing.

In the event the spillage is to the remote terminal at Building 101, the operator will take immediate action to safeguard any data. The following action will be exercised:

a. Material will be double wrapped and returned to the AIPRL operation manager via the next scheduled messenger service the same day.

(Continued)

b. If the spillage occurs beyond the limits of the service, then the material is to be stored in a specific container at the Building 101 Main Control Center which is under continuous guard control. On the next working day the material must be placed into the messenger service and returned to the AIPRL operations manager.

5.3.3 Passwords

Passwords are inherent to the software systems and generally will be protected from unauthorized personnel. However if a suspected compromise is discovered, it will be brought to the attention of the operations manager and the passwords will be changed. (Refer to Section 5.2.2.1.)

A compromise of a pasword will be treated as a security violation and will receive attention of the ADP Security Representative and the AIPRL operations manager as appropriate.

(b)(1)
(b)(3)

6.0 ADP SYSTEM OPERATIONS

6.1 MODES OF OPERATION

The AIPRL Computer Facility will have three modes of operation:

a. BYEMAN/TK

b. Unclassified

c. Special Category

The unclassified mode will be used when the security perimeter cannot be maintained, or when non-sensitive data is processed exclusively. Normally, the system will remain in the BYEMAN/TK mode (b)(1) during which time it will be processing TK and other data from (b)(3) several BYEMAN programs. Those persons having unescorted access to the computer room will have clearances for all major programs being supported by the Data Center, and all materials will be handled as appropriate for the highest security level information being processed.

Should the need arise to process customer classified data for a program not normally supported by the Data Center, a special category mode may be used when directed by an authorized customer representative. At this time no other data processing will occur.

6.2 SYSTEM PREPARATION - UNCLASSIFIED MODE

The following procedure will be used to initiate unclassified mode operations:

a. The operating system will be shut down, using the flush procedure which deletes temporary data sets, and writes unclassified data to all output devices. All vacant areas on the 3350 non-demountable disks shall be written over with unclassified data.

b. All classified tapes and disk packs will be demounted and stored.

c. A sign "unclass mode" will be placed in the TSO area.

6.2 (continued)

d. The sytem will be started using normal IPL procedures, as specified by the chief systems programmer. At this time only unclassified data processing may take place. Uncleared personnel will still require an escort. Appropriate warning light signs will be activated to inform all personnel of their presence in the area.

e. Upon termination, all unclassified materials and uncleared personnel will be removed from the computer room and TEMPEST integrity checked before any classified data processing resumes.

6.3 SYSTEM PREPARATION FOR SPECIAL MODE

The following procedure will be used to initiate special mode operations: (b)(1) (b)(3)

a. The operating system will be shut down using the flush procedure.

b. All tapes and disk packs, except those to be used, will be demounted and stored.

c. The terminal controller and communications controller to any RJE station will be turned off within the computer room.

d. The system will be started using normal IPL procedures. Access to the data center will be limited to thoseindividuals specified by the customer security representative.

e. Upon termination, all tapes and other materials used will be removed. The system will be flushed, shutdown, and restarted before normal data processing resumes.

7.0 AUDIT TRAILS

SMF data will be written to magnetic tape daily. This data will be analyzed to produce management usage reports and "security alert" reports. The latter will report exceptional behavior such as a user requesting a sensitive and unclassified tape on the same job, repeated abnormal terminations by a user, and other such conditions to be determined by the ADP Security Officer.

(b)(1)
(b)(3)

8.0 DOCUMENTATION

The AIPRL operations manager or his delegate, will maintain a record of all vendor-supplied software products currently installed, their revision level, and patches installed. In addition, he will maintain a library of vendor supplied documentation manuals, operational procedures, and documentation for system support programs (e.g., billing, security alert, etc.)

Individual users will maintain the documentation of their programs. The extent of such documentation will depend upon the "generality" and expected life of these programs. Documentation of user-programs of general interest may be added to the library.

(b)(1)
(b)(3)

9.0 CONTINGENCY PLANNING

9.1 BACKUP

User and system disk data sets will be routinely copied to magnetic tape backup on a three generation basis. At least one generation will be stored in a vault in a different building, as will a copy of the operating system.

(b)(1)
(b)(3)

9.2 RECOVERY

There is no plan to provide emergency data processing at an alternate site in the event of catastrophe.

9.3 EMERGENCY CLOSING

In the event of life-threatening disaster such as fire, earthquake, or civil disorder, the operators will trip emergency power shutoffs and close the doors as they leave. Security personnel will attempt to control re-entry. If time permits, classified tapes, disk, and printouts should be locked in their normal containers, before operators leave.