~~SECRET~~

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE
SUBJECT TO CRIMINAL SANCTIONS

BIF-008-WA-000170-OH-86
This document contains 33 pages
Copy 001 of 009 copies
DATE: 16 June 1986

ADP NETWORK SYSTEM SECURITY PLAN

FOR

ADVANCED IMAGE PROCESSING AND

RECORDING LABORATORY (AIPRL)

HAWK EYE PLANT

PHASE I

T. H. Daniels
ADPSSR

R. D. Sherwood
General Manager

(b)(3)

BIFSCO

-WARNING-
'THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

DERIVATIVE CL BY: BYE-1
DERIVED FROM: BYE-1
DECLASSIFY ON: OADR

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT'D)

LIST OF FIGURES

I. INTRODUCTION

This ADP System Security Plan describes the security measures in effect for Phase I of the Advanced Image Processing and Recording Laboratory (AIPRL) network located on the first (ground) floor of Building 2, at the Eastman Kodak Company, Hawk Eye Plant, 20 Avenue E, Rochester, NY 14650. The components for the Phase I network, residing within the AIPRL are: a "VAX Cluster" consisting of the Image Display Station 1 (IDS-1), VAX 11/785, and Image Display Station 2 (IDS-2), VAX 8600 Systems, DEC ETHERNET Package, DECNET Package, and the APTEC-1 and APTEC-2 I/O computers (IOC's).

The IDS-1 (VAX 11/785) is located in Room 2-1-2, with image display stations and terminals located in Rooms 2-1-1, 2-1-3, and 2-1-4 of Building 2. These four rooms measure a total of 37 feet by 13 feet (See Figure 1).

The IDS-2 (VAX 8600) is located in Room 2-1-5 of Building 2. This room measures 46 feet by 38 feet (See Figure 1). Terminals for the IDS-2 are located in Room 2-1-1 of Building 2 (See Figure 1). Also residing in the AIPRL, but operating as separate and independent nodes are: (a) IBM 4341 (DPC) located in Room 2-1-5, (b) VAX 11/750 (SL) located in Room 2-1-9, and (c) MICRO VAX (LWD) located in Room 2-1-8 (See Figure 1).

II. ADP SYSTEM SECURITY RESPONSIBILITY

As designated by the Eastman Kodak Company Byeman Industrial Facilities Security Control Officer (BIFSCO), Mr. Thomas H. Daniels is the ADP System Security Representative (ADPSSR) on a full-time basis for the AIPRL. Mr. Daniels reports directly to [redacted] BIFSCO, and can be reached via telephone on (716) 436-3586 or secure 00141 (716) 436-5054. Mr. Walter K. Koopman is the Facility Security Representative (FSR) for Hawkeye Plant (See Figure 2). (b)(3)

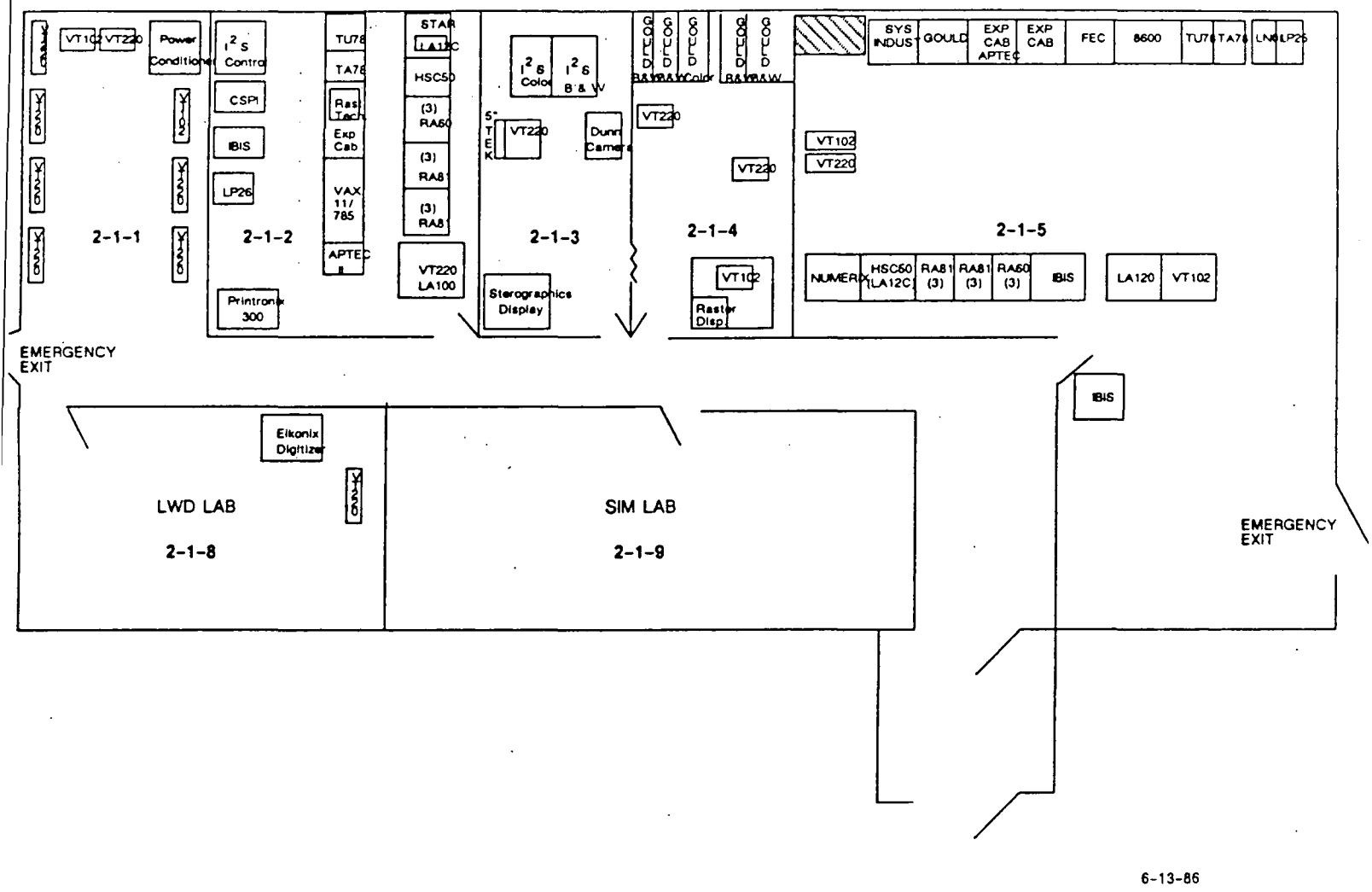
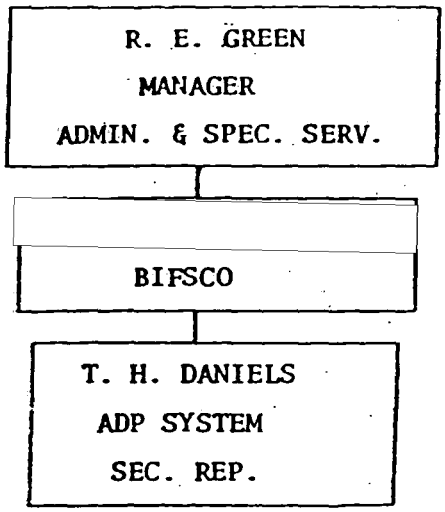


Figure 1. IDS-1 and IDS-2 Floor Plan



(b)(3)

Figure 2. ADP System Security Organization

III. SYSTEM ENVIRONMENT

AIPRL is within a TEMPEST enclosure located on the first (ground) floor of Building 2 in the North quadrant of an approved SCIF within the Hawk Eye Plant (see Figure 3). The TEMPEST enclosure was tested to MIL-STD-285 and NSA65-2, and certified by Program B Message 6835 dated 19 April 1980, recertification of the enclosure will be in 1986. AIPRL is also approved for open-shelf storage by Program B Message 4020 dated 10 June 1983. Program B holds security cognizance for the AIPRL facility

IV. SYSTEM SECURITY

A. MODE OF OPERATION

The Phase I configuration for the two VAX nodes and associated peripherals operates in the System High Mode (for two or more NFIB members) as defined in Paragraph V.A.2, SCIREQ 84, dated August 1984.

The Phase I configuration processes data for more than one customer, and is dedicated to process NRO sponsored multi-program sensitive compartmented information, up to and including TOP SECRET Byeman and TK. Unclassified program related software development activity is approved for this configuration by the Contracting Officers Technical Representative (COTR).

B. PERSONNEL ACCESS CONTROLS

1. The Phase I configuration is accessed by approximately 130 system users. These users require unescorted access to the network and are security approved according to DCID 1/14 standards and are access approved for all SCI programs.

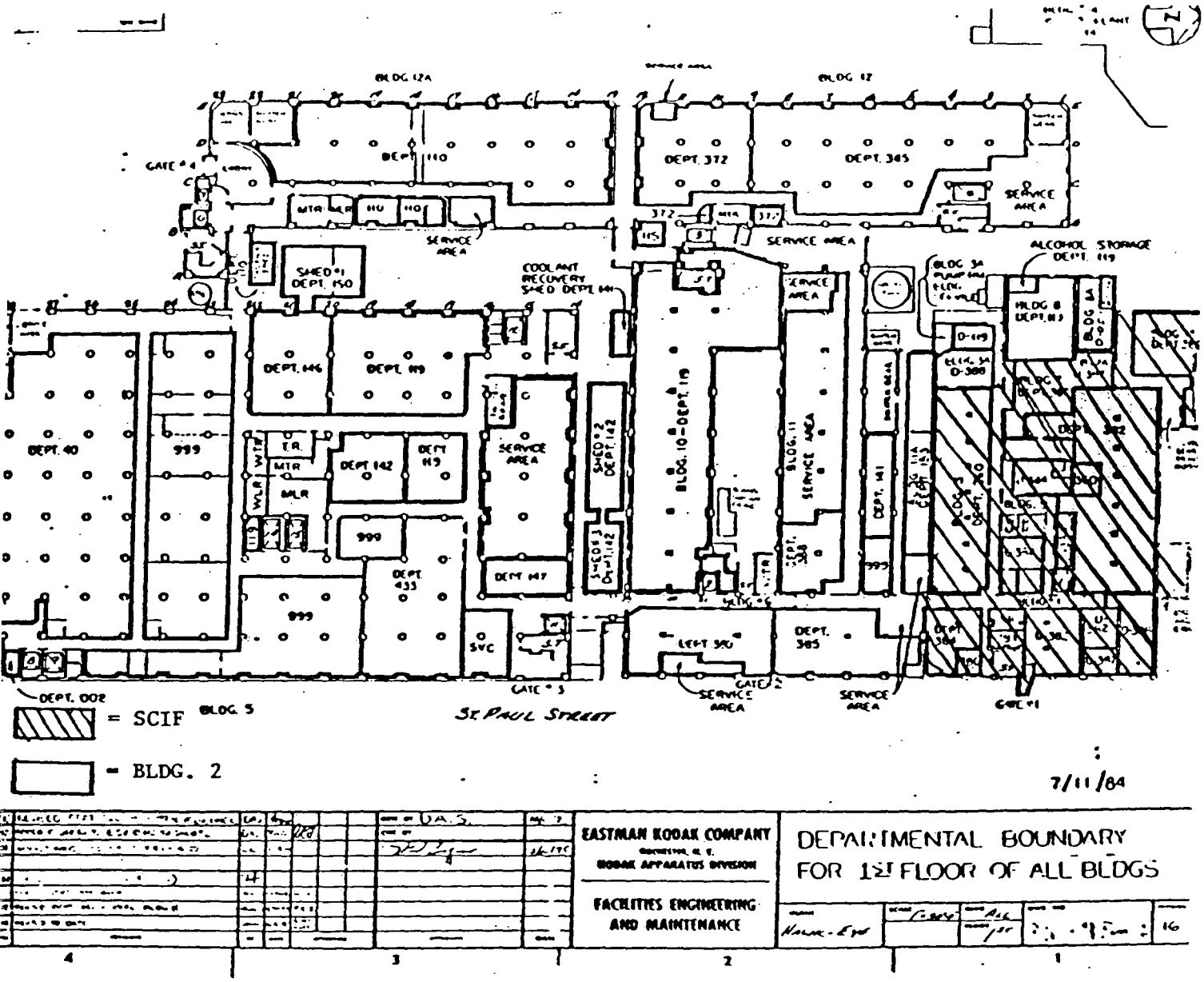


Figure 3. Hawk Eye Floor Plan

~~WARNING~~

"THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

~~SECRET~~ HANDLE VIA BYEMAN CONTROL SYSTEM ONLY

2. Need-to-know is established by the appropriate EK Project Manager, and access must be confirmed by an appropriate indicator on the individuals area badge.

3. Except for downtime periods, there is a minimum of two cleared individuals present in the AIPRL and the rooms in which terminals are installed; and two individuals are required to open and close the AIPRL.

4. Access to the individual rooms within the AIPRL is via simplex locks installed at the entrance door of each room.

5. All visitors to the AIPRL must be identified and a visitor log is kept in the office of the FSR.

6. All visits by uncleared personnel must be approved on a case-by-case basis by the FSR, and the following actions are taken:

   a. All sensitive material is secured in an approved security container.

   b. An "Uncleared Visitor in Area" sign is placed on the door of the room being visited.

   c. A flashing colored light is placed in the corridor outside the room being visited.

   d. The uncleared visitor is met at the plant entrance by an Customer-approved individual and is kept under constant escort throughout the visit.

e. The uncleared visitor is escorted back to the plant entrance at the end of the visit.

C. PHYSICAL SECURITY

1. Hawk-Eye Plant:

a. The Hawk-Eye Plant is completely surrounded by barbed-wire topped eight (8) foot chain link fence.

b. Eastman Kodak Company uniformed guards are stationed at the three (3) plant entrances. The main entrance, only, is open and manned twenty-four (24) hours per day.

2. Hawk-Eye SCIF:

a. Entry to and egress from the SCIF is through a twenty-four (24) hour per day guard post manned by a minimum of two (2) Customer-approved, Eastman Kodak Company uniformed guards utilizing a color coded badge exchange system.

3. AIPRL:

a. Entry to and egress from the AIPRL main entrance is controlled by an electronic cypher unit. For downtime purposes, the AIPRL entrance is also secured with an S&G safe-master extension 50 locking device.

4. Alarms:

a. The AIPRL doors are equipped with magnetic contact door alarm switches, Class "A" alarm system.

b. An advisor VIII high security ultrasonic motion detector system is used for the entire AIPRL.

NOTE: All alarms are connected to the Wells Fargo annunciator system located at the 24 hour guard post (see Paragraph C.2.a, above).

D. SYSTEM HARDWARE

1. The system hardware associated with the Phase I configuration is listed in Figure 4 by manufacturer, model number, serial number, memory size, and memory type. The system configuration (functional diagram) is shown in Figure 5. The security features of the VAX 11/785 and VAX 8600 are:

a. Volatile memory (i.e., no residual memory exists when power to units is turned off). The VAX 8600 does have a battery back-up, to prevent loss of data during a power outage.

b. Memory bounds mechanism which prohibits system users from reading/writing in memory occupied by the Operating System or other system users.

VAX - 11/785 EQUIPMENT LIST

MANUFACTURER	DESCRIPTION	MODEL #	SERIAL #
2-1-1			
DIGITAL	CRT W/KEYBOARD	VT220	TA01646
DIGITAL	CRT W/KEYBOARD	VT220	TA04334
DIGITAL	CRT W/KEYBOARD	VT220	ABAR393
DIGITAL	CRT W/KEYBOARD	VT220	TA044849
DIGITAL	CRT W/KEYBOARD	VT220	TAF6102
DIGITAL	CRT W/KEYBOARD	VT220	TAF6156
DIGITAL	CRT W/KEYBOARD	VT220	TA04129
DIGITAL	CRT W/KEYBOARD	VT102	TA04104
DIGITAL	CRT W/KEYBOARD	VT102	TAF6219
LIEBERT	ELEC. POWER UNIT	LRC30	85255A
2-1-2			
INTER.IMAGING SYS	IMAGE PROCESSOR(12S)	70	
CSPI INC.	ARRAY PROCESSOR	MAP310	1549
IRIS	DISK DRIVE	1400TF	519
DIGITAL	PRINTER	LP26EA	C46369-B600
PRINTRONICS	PRINTER	P300	469128
DIGITAL	TAPE DRIVE	TA78-BF	SP11466
DIGITAL	TAPE DRIVE	TA78-AF	SP13236
RASTER TECH.	DISPLAY DRIVER	80	RT00349
DIGITAL	CPU-EXP.CAB.(APTEC)	H9652-MA	FX02323
DIGITAL	CPU	11/785	FXA0807
APTEC	COMPUTER IOC	IOC2400	8542002
DIGITAL	STAR COUPLER	SC008-AB	
DIGITAL	DISK/TAPE CONTR.	HSC50-AA	CX02191
DIGITAL	SYSTEM PRINTER	LA120	PN67756
DIGITAL	DISK DRIVE	RA81-EA	CX89665
DIGITAL	DISK DRIVE	RA81-EA	CX89609
DIGITAL	DISK DRIVE	RA81-EA	CX89613
DIGITAL	DISK DRIVE	RA81-EA	CX89457
DIGITAL	DISK DRIVE	RA81-EA	CX89420
DIGITAL	DISK DRIVE	RA81-EA	CX89414
DIGITAL	DISK DRIVE	RA60-EA	CX02817
DIGITAL	DISK DRIVE	RA60-EA	CX02623
DIGITAL	DISK DRIVE	RA60-EA	CX03318
DIGITAL	CRT W/KEYBOARD	VT220	TA37849
DIGITAL	SYSTEM PRINTER	LA100	PN59395
2-1-3			
CONRAC	MONITOR (B&W)	QQA17/Y	523134
CONRAC	MONITOR (CLR)	7311C19	510332
DIGITAL	CRT W/KEYBOARD	VT220	TAF6147
STEROGRAPHICS	MONITOR (B&W)		
DUNN/TEKTRONIX	CAMERA SYSTEM	631	253
AREAS 2-1-4 & 2-1-8 CONTINUED ON NEXT PAGE			

Figure 4. System Hardware

MANUFACTURER	DESCRIPTION	MODEL #	SERIAL #
2-1-4			
AMTRON	GOULD MONITOR	CD1909-2	IHE17-6-001
COMU	GOULD MONITOR	9617/C	133226
MITSIBICHI	GOULD MONITOR	M6950	2100157
MITSIBICHI	GOULD MONITOR	M6950	2100143
SONY	GOULD MONITOR	GRM1901-12	200138
TEKTRONICX	RASTER DISPLAY	634	B010198
DIGITAL	CRT W/KEYBOARD	VT220	TAF6400
DIGITAL	CRT W/KEYBOARD	VT220	TAF6361
DIGITAL	CRT W/KEYBOARD	VT102	ABAE322
2-1-8			
FIKONIX	DIGITIZER	785	23
DIGITAL	CRT W/KEYBOARD	VT240	Y4F-052866

VAX - 8600 EQUIPMENT LIST (2-1-5)

MANUFACTURER	DESCRIPTION	MODEL #	SERIAL #
DIGITAL	CPU	KA86-AA	MR01482
DIGITAL	CPU-FRONT END CAB.	KA86-AA	MR01482
DIGITAL	CPU-EXP.CAB.(APTEC)	H9652-FA	AS01005
NUMERIX	ARRAY PROCESSOR	H9642CA	WF52205875
APTEC	COMPUTER IOC	IOC2400	8542001
GOULD DEANZA	IMAGE PROCESSOR	IP8500	68023
DIGITAL	CONSOLE PRINTER	LA12C	PN13175
DIGITAL	CONSOLE PRINTER	LA120-DA	PNU4865
DIGITAL	LASER PRINTER	LN01-AC	G76010297
DIGITAL	PRINTER	LP25	26N15201
DIGITAL	HSC50	HSC50-AA	CX05122
DIGITAL	DISK DRIVE	RA81-EA	CX85685
DIGITAL	DISK DRIVE	RA81-EA	CX86803
DIGITAL	DISK DRIVE	RA81-EA	CX86660
DIGITAL	DISK DRIVE	RA81-EA	CX85833
DIGITAL	DISK DRIVE	RA81-EA	CX86009
DIGITAL	DISK DRIVE	RA81-EA	CX86613
DIGITAL	DISK DRIVE	RA60-EA	CX04210
DIGITAL	DISK DRIVE	RA60-EA	CX04181
DIGITAL	DISK DRIVE	RA60-EA	CX04243
IBIS	DISK DRIVE	1400	649
IBIS	DISK DRIVE	1400	650
DIGITAL	TAPE DRIVE	TA78-BF	SP11335
DIGITAL	TAPE DRIVE	TU78-AF	SP09595
SYSTEM INDUSTRIES	TAPE DRIVE	9700-53	8264
DIGITAL	CRT W/KEYBOARD	VT220	TA03970
DIGITAL	CRT W/KEYBOARD	VT102	ABAR495
DIGITAL	CRT W/KEYBOARD	VT102	TA07278

Figure 4A. System Hardware Continued

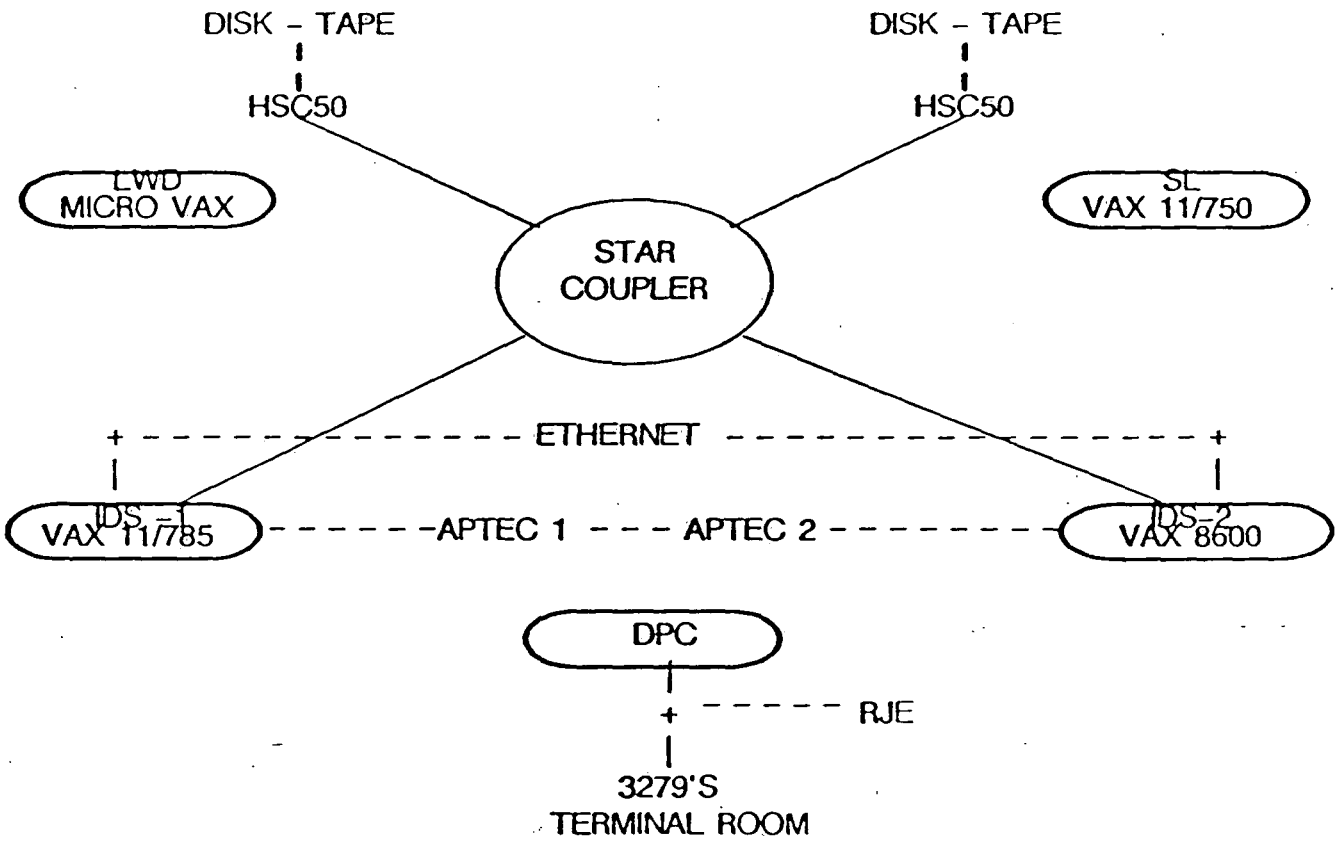


Figure 5. System Configuration

c. The system has two classes of machine instructions. One class is for the exclusive use of the Operating System. The other class is usable by both the Operating System and approved applications programs.

d. A time-of-day clock is utilized for the recording of system activity, particularly the creation of printed output.

E. SYSTEM SOFTWARE

1. The operating system utilized by both nodes of the Phase I configuration is an unmodified VAX/VMS Release 4.4.

2. The VAX/VMS Operating System:

a. Supports all VAX computers, working reliably and efficiently in both time-sharing and production environments.

b. On erroneous input, the user receives a message.

c. On a power failure, the system shuts down automatically.

d. Provides privilege, protection, and quota mechanisms to limit user access to system-controlled structures in physical memory, system-structured files and volumes, and certain devices.

e. Maintains user accounts in a user authorization file which constitutes the basis for privilege and quota assignments.

f. Includes a break-in detection which allows terminals to be disabled when a break-in attempt is detected.

g. Utilizes a user identification code (UIC), on which the protection mechanism is based.

h. Has scavenge protection, provided in three forms:

(1) File high-water marking which prevents users from reading beyond the end of a file mark.

(2) Erase on delete which insures that information in a file is zeroed before being returned to general use.

(3) Erase on extend which prevents a user from reading information that may have been previously allocated to another file.

F. SYSTEM ACCESS CONTROLS

1. Each node in the Phase I configuration operates from a common system disk to ensure that the account and access control privileges do not differ from node to node. This common Access Control List (ACL), User Authorization File (UAF), Rightslist File performs a function similar to the capability of the ACF2 security package.

2. Prior to being allowed access to the Phase I network, each user is identified as Customer-approved and possessing an established need-to-know for data associated with the network.

3. System logon passwords are individual user unique pronounceable identifiers no less than 6 characters and no longer than 8 characters in length.

4. System logon passwords are randomly selected from a Customer-supplied listing of acceptable system logon passwords. The listing, and the assigned system logon passwords are controlled by the Facility Security Representative (FSR) and one alternate individual specifically designated by the FSR.

5. Knowledge of the system logon passwords is restricted to the individual system user, the FSR, and the designated alternate to the FSR.

6. System logon passwords are changed every six (6) months.

7. Appropriate system logon passwords will be changed whenever an actual or suspected system compromise occurs, or whenever a system user leaves the project.

8. The number of system logon password entry failures allowed a system user attempting to access any AIPRL system is limited to three (3). A user who exceeds this limitation is automatically denied access to the system and his/her access must be reactivated by the FSR.

G. DATA AND PROGRAM STORAGE MEDIA

All data and program storage media are assigned a document control number by the Document Control Office (DCO), and are labeled, handled, and stored at the highest security classification level of the information ever recorded on them. Any requested exception shall be approved, in writing, by the Customer's Information Systems Security Officer (ISSO).

1. Identification/Labeling:
   This activity is performed only by specifically designated personnel in cooperation with the FSR and in accordance with applicable Customer directives.

   a. Magnetic tapes, disk packs, floppy disks, and cassettes are affixed with a label to indicate clearly the highest security classification level and SCI control channel(s) of the information ever contained on them, together with the appropriate document control number.

   b. Card decks and program listings are manually labeled in accordance with applicable Customer directives to indicate clearly the highest security classification level and SCI control channels(s) of the information contained on them, together with the appropriate document control number.

2. Transportation:
   Whenever removable magnetic data and program storage media, card decks, or program listings are required to be taken outside the SCIF, at least two Customer-approved individuals accompany the material. A receipting method is used to ensure that accountability is maintained.

3. Accountability:
   Specific Customer-approved individuals are designated, and readily identifiable on an access list maintained by the FSR, to receipt for all classified removable data and program storage media, card decks, and program listings. All classified media are accounted for using an accountability system approved by the Customer.

4. Sanitization Procedures:

The following sanitization procedures are used:

a. Regular Magnetic Tapes:

(1) Regular magnetic tapes (i.e., magnetic tapes having a coercivity of 325 oersteds or less) are degaussed using a Customer-approved Bell and Howell, Model TD-290343, magnetic tape degausser; the label identifying the highest security classification and SCI control channel(s) of the information ever recorded on them is not removed.

(2) When magnetic tapes become unusable, they are destroyed by the FSR in accordance with applicable Customer directives and Customer-approved procedures. Receipts and logs of this activity are maintained in the DCO.

b. Fixed Disk Units:

Fixed disk units are sanitized using a Customer-approved, overwrite routine only after receiving written approval from the ADPSSR and assurance that this approval has been coordinated with the Customer's ISSO. If one of these units becomes no longer usable, the platters will be removed and destroyed in accordance with applicable Customer directives and specific instructions received from the Customer's ISSO.

c. Floppy Disks:

Floppy disks are not sanitized. When these storage devices become unusable, they are destroyed in accordance with applicable Customer directives.

d. Internal Memory:

Each network CPU employs semiconductor volatile internal memory. The power OFF procedure is used for sanitization.

H. AUDIT TRAILS

The audit trail records implemented utilize both automated and manual techniques.

1. Automated Audit Trail:

The automated records made available by both the VAX 11/785 and the VAX 8600 are fully utilized. The DEC Net Log provides date and total access times by User ID; and it records successful and unsuccessful attempts to SET HOST and access host and node data files. The ACL Log records successful and unsuccessful attempts to access host and node data sets, and the Operator Communications Log records all other user activity and provides the security-related alarms described in Paragraphs IV.D and IV.E, above.

These automated records are printed and reviewed daily by the Computer Facility Security Officer (CFSO), and maintained for one (1) year. Any irregularities are brought to the attention of the Facility Security Representative and the ADPSSR.

2. Manual Audit Trail:

a. Visitors Log: Used to record each visitor's name, date, and time of visit, and the name of the visitor's escort for the area.

b. Open/Close Log (Figure 6): Used to identify individuals who close/open the computing facility by date and time.

c. Computer Center Security Checklist (Figure 7): Used to identify and verify all procedures required for system start-up, processing, and shut-down operations.

d. Hardware Maintenance Log: Used to identify and maintain computer system hardware changes, identify maintenance problems, identify individual performing maintenance operations, identify assigned escort, identify exactly what maintenance is performed, and assess potential security impacts.

e. Software Configuration Control Log (Figure 8): Used to identify all software available to the system.

f. Transportation Receipt (Figure 9): Used to provide traceability for material being transmitted from one approved area to another approved area in accordance with Customer requirements.

g. Document Transaction Card (Figure 10): Used to record receipt, accountability, and destruction of all accountable material in accordance with Customer requirements.

I. DOCUMENTATION

Designated systems personnel possess/maintain a complete set of systems, operations, user, and program documentation in Room 1-1-12. This information is available for use by any individual who is customer-approved for unescorted access to the network.

SECURITY CONTAINER RECORD SHEET

Month_____ Container No._____ Location_____ Area_____ Plant_____
floor-bldg.

DATE	OPENED TIME	BY	CLOSED TIME	BY	CHECKER GUARD TIME	BY	TIME	BY
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								

Instructions person opening and closing container and the security inspector will enter appropriate time and initial.

Figure 6. Open/Close Log

~~WARNING~~

"THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

CHECKLIST FOR PREPARATION, PROCESSING, AND TERMINATION OF PROCESSING OF &*&&Z$& INFORMATION

Preparation: Date _____ Time _____ Initials _____/_____

_____ 1) Nofity users that the system is shutting down for classified processing.

_____ 2) Clear all unauthorized personnel from the computer room/terminal room.

_____ 3) Shut the system down with the SHUTDOWN software routine and HALT the CPU.

_____ 4) Shut the CPU off and leave off for five (5) minutes, MINIMUM.

_____ 5) Remove the system disk from the drive and secure.

_____ 6) Remove the boot floppy from the drive and secure.

_____ 7) Spin down,
write protect,
disable port select button and
remove unit number plug from the additional drive(s) that are not to be used during the classified processing period.

_____ 8) Disconnect cluster communication cables at the back of the CPU cabinet (CAREFULLY!!).

_____ 9) Disconnect remote I/O devices at the patch panel.

_____ 10) Disconnect all local I/O devices at the device.

_____ 11) Disconnect the CPU from the Ethernet at the CPU.

_____ 12) Insert &*&&Z$& boot-up floppy.

_____ 13) Insert &*&&Z$& user/system disk.

_____ 14) Boot the system at the console.

Processing: Date _____ Time _____ Initials _____/_____

_____ 15) Monitor system access at console.

_____ 16) If a security-related, abnormal processing operation occurrs involving any storage media, stop processing and contact Tom Daniels, extension 32328.

_____ 17) If processing is to continue, reboot the system at the console.

_____ 18) Log all security-related abnormal system operations/security violations and report them to Tom Daniels, extension 32328.

_____ 19) In an emergency, secure the doors as you leave and activate the alarms. If time permits, secure demountable data and program storage media. Contact Tom Daniels, extension 32328, as soon as practical.

Termination: Date _____ Time _____ Initials _____/_____

_____ 20) Dump all accountability/activity files to demountable storage media.

_____ 21) Shut the system down with the SHUTDOWN software routine and HALT the CPU.

_____ 22) Remove the &*&&Z$& user/system disk from the drive.

_____ 23) Remove the &*&&Z$& boot floppy from the drive.

_____ 24) Shut the system off and leave off for five (5) minutes, MINIMUM.

_____ 25) Shut printer(s) used during processing period off and leave off for five (5) minutes, MINIMUM.

_____ 26) Return &*&&Z$& disk to the designated custodian.

_____ 27) Place all classified waste, notes, listings, working papers, and printer ribbons requiring destruction in the special burn container.

_____ 28) Return system to normal operation.

Figure 7. Computer Center Security Checklist

SOFTWARE

VAX 11/785 - IDS AREA

Manufacturer	Description
[redacted]	
ISSCO	DISSPLA Graphics V10.0
International Math & Statistics Library, Inc.	IMSL Library
Could/DeAnza	LIPS Digital Image Processing Software V1.0
I^2S	System 570 Image Processing Software
Raster Technologies	ONE/80 Software Lib.
CSPI (Array Porcessor)	SNAP II Software, Extended Arithmatic Function Library V3.0
Penn State Univ.	Mini-tab Software
[redacted]	
Aptec	Staple - Driver Software
Numerix (MARS 425)	Arex - Avid (Fortran Devel. Sys.)

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

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

Figure 8. Software Configuration Log

TRANSMITTAL RECEIPT No.118002

Materials Received: _____ (From) _____ (Channel/Number) _____ (Station) _____ (Date)

Description of Contents:

☐ Class.
☐ Uncl.

Transmittal Authorized By: _____ (Signature) _____ (Date)

Description of Package, Envelope, Etc.:

From: _____ (Control Station) To: _____ (Control Station) For: _____ (Individual)

Signature Receipt(s) and Date(s):

1) _____ _____ 4) _____ _____

2) _____ _____ 5) _____ _____

3) _____ _____ 6) _____ _____

RE 3157 (8-74) LAST ENTRY SHOULD BE CROSS REFERENCED TO SUBSEQUENT CONTROL SYSTEM

REMOVE TAPE FROM BACK AND ATTACH FORM TO ENVELOPE.

MCP ® MOORE BUSINESS FORMS, INC. PATENT 3,429,827

Figure 9. Transportation Receipt

~~WARNING~~

"THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

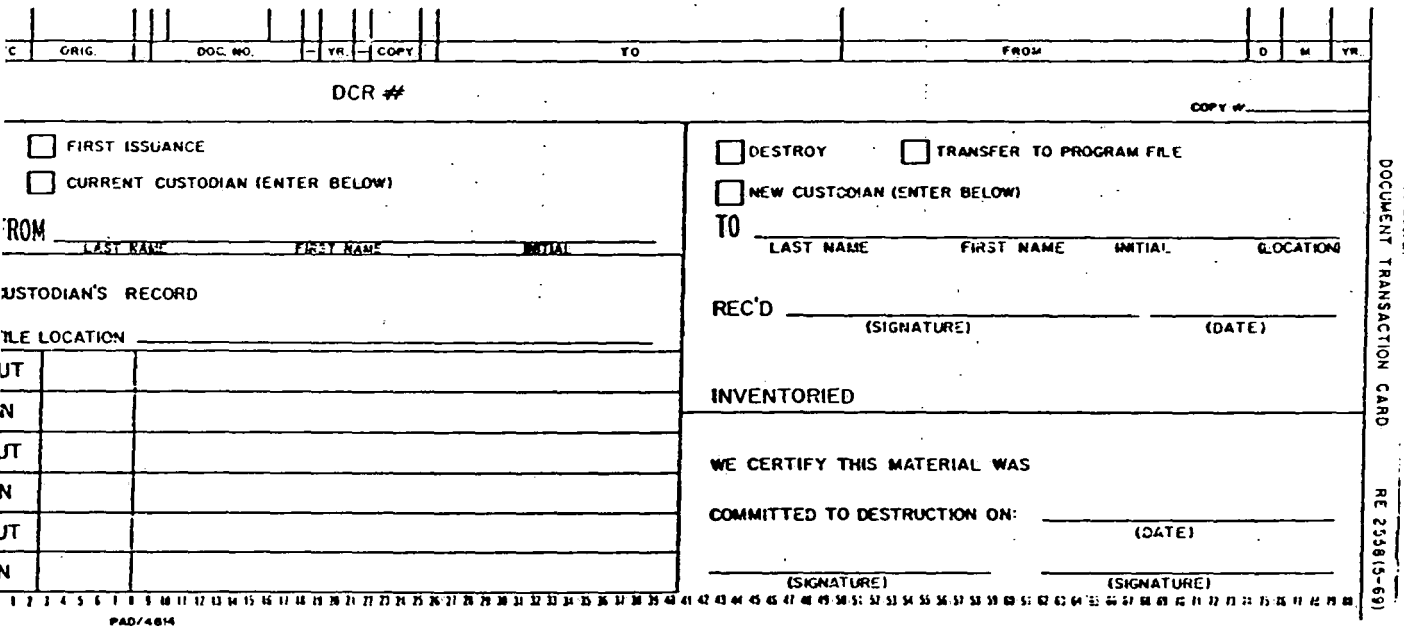


Figure 10. Document Transaction Card

~~WARNING~~

"THIS DOCUMENT SHALL NOT BE USED AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

J. STORAGE AREAS

Storage of classified magnetic media (fixed disks, removeable disks, and tapes) is in Rooms 2-1-2 and 2-1-5, which are approved for open-shelf storage. Floppy diskettes, cassettes, hard copy output, and documents are stored in Customer-approved storage containers located through the AIPRL. Combinations for those containers are changed once a year or upon transfer/debriefing of an individual having knowledge of the combinations.

K. COMMUNICATIONS LINKS

Physical disconnects of I/O devices or any direct memory access devices external to the network, but within the AIPRL facility, are provided by the use of switching devices. The [redacted] ETHERNET capability provides node to node communications and terminal communications within the network via COMSEC approved fiber optic links. There are no telecommunication capabilities in place or planned. (b)(1) (b)(3)

L. EMANATIONS

The AIPRL facility is constructed and approved per NSA-65-6 specifications, and received TEMPEST certification from the Customer's communication security (COMSEC) authority via program B message 6835, dated 19 April 1980.

V. ADP SYSTEM OPERATIONS

A. SYSTEM PREPARATION AND INITIALIZATION PROCEDURES

Prior to processing classified information, the following actions are completed by systems support personnel.

1. All unauthorized personnel are cleared from the computing facility.

2. Those I/O devices and direct access storage devices not to be used during processing operations are taken off-line. Only those terminals designated for use during processing operations remain connected.

3. All demountable and program storage media not to be used during the scheduled processing are removed from the system and placed in approved storage containers.

4. The CPU's internal memory is sanitized using the power OFF procedure.

5. The dedicated version of the Operating System, including other attendant software, is loaded onto the system and the system is initialized for processing.

B. DATA PROCESSING

1. Security measures in effect during all processing periods are commensurate with the handling of material at the Top secret classification level.

2. During normal working hours, a minimum of two (2) security approved individuals are present in the computing facility during classified processing. When unattended processing occurs during downtime, the computing area is secured and entry/egress is controlled by the monitoring of the alarms by guards stationed at the entrance to the SCIF.

3. Verification of terminal utilization, system user logon entries, and file access approvals of system users is performed by the system.

4. If a security-related, abnormal processing operation occurs involving any storage media (i.e., system compromise or data spillage), processing is stopped and the ADP Systems Security Representative is contacted for determination of action to be taken.

5. If processing is to continue, the dedicated version of the Operating System is reloaded and the system reinitialized.

6. All security-related abnormal system operations and security violations are logged and reported to the Contracting Officers Security Representative (COSR) and the Customer's ISSO via the ADP Systems Security Representative.

7. Should an act of nature or civil disturbance occur, or threaten to occur, the system operators will secure the doors and activate the alarms as they leave. If time permits, demountable data and storage media will be secured in approved storage containers. The ADP Systems Security Representative will be notified, and in turn will notify the Customer's ISSO, as soon as practical.

C. OUTPUT CLASSIFICATION/HANDLING PROCEDURES

Output produced during classified processing is collected by the user(s). It is the user's responsibility to insure that all material is properly classified (i.e., labeled, assigned a control number). Any output not collected by the end of the day is collected by opera-

tions personnel, separated by user ID and secured in an approved storage container. If the user has not claimed the output within two days, it is destroyed in accordance with applicable customer directives.

D. MODE TERMINATION

Upon completion of processing, the following actions are taken:

1. All accountability/activity files are dumped to demountable storage media.

2. A Shut-down program initiated to remove all users and shut down the system.

3. Operators remove all demountable data and program storage media from the system used during the classified processing period, including the dedicated version of the Operation System.

VI. SYSTEM MAINTENANCE

A. Uncleared maintenance representatives are monitored at all times by a Customer cleared individual who is technically knowledgeable of the system or component being maintained.

B. All classified media are properly secured and the room/location of the maintenance activity is visually inspected prior to the visit.

C. A visitor log is signed by the maintenance representative and by the project-assigned escort prior to entering the SCIF.

D. Tool boxes and materials belonging to the maintenance representative are inspected by the assigned escort before being taken into the SCIF. Any communication devices and any magnetic media not required for the maintenance visit are retained at the guard desk at the entrance to the SCIF.

E. All software/firmware required for maintenance of diagnostics are maintained within the AIPRL and stored and controlled as though classified. Maintenance representatives are not allowed to remove any magnetic media from the AIPRL.

F. Malfunctioning circuit boards having certified volatile memory may be released from the AIPRL for factory repair only after approval of the Customer's ISSO.

G. Malfunctioning circuit boards having nonvolatile memory components may be released from the AIPRL for factory repair only after verification by the Customer's ISSO that all memory components are completely sanitized.

H. A maintenance log is maintained. Whenever maintenance personnel visit the AIPRL, the name of the individual, the name of the assigned escort, specific maintenance performed, and the date and time are recorded in the log.

I. Remote diagnostics are not utilized for maintenance purposes. Approval from the Customer's ISSO will be requested in advance should the use of remote diagnostic links come under consideration.

J. If required, a separate copy of the dedicated version of the appropriate operating system is made available for maintenance activity.

VII. SECURITY EDUCATION

All Eastman Kodak Company personnel who work in the secure area are provided a security awareness briefing when assigned to the project and every year thereafter. Individual responsibilities are disseminated at these must-attend briefings given by the ADP Systems Security Representative before access to any system within the AIPRL is granted.