

~~SECRET~~

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE
SUBJECT TO CRIMINAL SANCTIONS

BIF-008 W-A-000036-OH-87
This document contains 1 pages
Copy 4 of 009 copies
Date 31 March 1987

To: D. Anderson



J. Moore

(b)(3)

From:  T. H. Daniels

(b)(3)

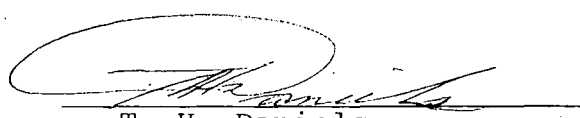
Subject: IBM-4341 Installation and Operation Within a SCIF

Reference: (A) Security Requirements for Contractor Automated
Information Systems Processing SCI, Dated August
1984

Enclosure: (1) Security Plan for IBM-4341 Data Processing Center
(DPC) Dated 31 March 1987 (BIF008-WA-000034-OH-87)

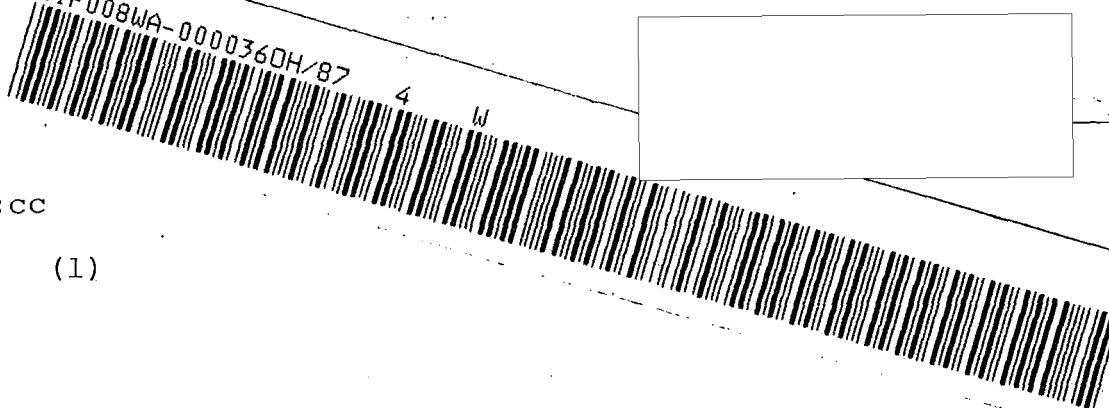
Reference (A) sets forth specific security requirements for the operation of ADP equipment within secure program areas and stresses that prior to equipment installation and operation, a system security plan must be approved by the customer.

BIF008 hereby submits enclosure (Security Plan for IBM-4341) for your consideration and approval. We request final authorization to operate the IBM-4341 as described.


T. H. Daniels

(b)(3)

BIF008WA-000036OH/87



DAS:cc

Enc. (1)

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

~~SECRET~~

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

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

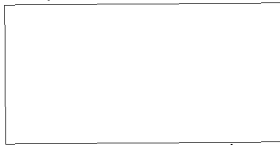
~~SECRET~~

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE
SUBJECT TO CRIMINAL SANCTIONS

BIF-008-WA-000046-OH-87

This document contains 1 pagesCopy 3 of 9 copiesDATE: May 4, 1987

To:



J. Moore

(b)(3)

From:



T. H. Daniels

(b)(3)

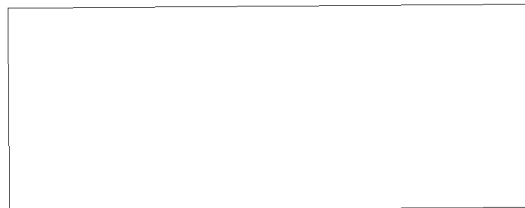
Subject: Network Installation and Operation Within a SCIF.

Reference: (A) Security Requirements for Contractor Automated Information
Systems Processing SCI, Dated August 1984Enclosure: (1) ADP Network System Security Plan Phase II Hawkeye Plant,
(BIF-008-WA-000047-OH-87)

Reference (A) sets forth specific security requirements for the operation of
ADP equipment within secure program areas and stresses that prior to equipment
installation and operation, a system security plan must be approved by the
customer.

BIF008 hereby submits enclosure (System Security Plan for Phase II Network)
for your consideration and approval. We request final authorization to
operate the Phase II (VAX Cluster) network as described.

T. H. Daniels



BIF008WA-000046OH/87

(b)(3)

~~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~~

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE
SUBJECT TO CRIMINAL SANCTIONS

~~SECRET~~

BIF-008-WA-000047-OH-87

This document contains 40 pages

Copy 3 of 9 copies

DATE: May 4, 1987

BIF008WA-000047OH/87 3 X



ADP NETWORK SYSTEM SECURITY PLAN

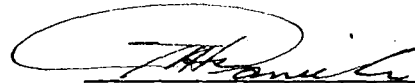
FOR


ADVANCED IMAGE PROCESSING AND

RECORDING LABORATORY (AIPRL)

HAWK EYE PLANT

PHASE II


T. H. Daniels
ADPSSR


R. D. Sherwood
General Manager



BIFSCO

(b)(3)

-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~~

~~SECRET~~

BIF-008-WA-000047-OH-87

TABLE OF CONTENTS

<u>Section</u>	<u>Title</u>	<u>Page</u>
	Title Page	1
	Table of Contents	2
	List of Figures	4
I	<u>INTRODUCTION</u>	5
II	<u>ADP SYSTEM SECURITY RESPONSIBILITIES</u>	6
III	<u>SYSTEM ENVIRONMENT</u>	6
IV	<u>SYSTEM SECURITY</u>	6
	A. MODE OF OPERATION	6
	B. PERSONNEL ACCESS CONTROLS	7
	C. PHYSICAL SECURITY	8
	D. SYSTEM HARDWARE	9
	E. SYSTEM SOFTWARE	10
	F. SYSTEM ACCESS CONTROLS	12
	G. DATA AND PROGRAM STORAGE MEDIA	16
	H. AUDIT TRAILS	18
	I. DOCUMENTATION	20
	J. STORAGE AREAS	21
	K. COMMUNICATIONS LINKS	21
	L. EMANATIONS	21

~~-WARNING-~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

TABLE OF CONTENTS (CONT'D)

<u>Section</u>	<u>Title</u>	<u>Page</u>
V	<u>ADP SYSTEM OPERATIONS</u>	21
	A. SYSTEM PREPARATION AND INITIALIZATION PROCEDURES	21
	B. DATA PROCESSING	22
	C. OUTPUT CLASSIFICATION/HANDLING PROCEDURES	24
	D. MODE TERMINATION	24
VI	<u>SYSTEM MAINTENANCE</u>	25
VII	<u>SECURITY EDUCATION</u>	26

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1	VAX Cluster Floor Plan	28
2	Distributed Terminal Connection	29
3	ADP System Security Organization	30
4	Hawk Eye Floor Plan	31
5	System Hardware	32
6	System Configuration	33
7	Project Directory Hierarchy	34
8	Open/Close Log	35
9	Computer Center Security Check List	36
10	Software Configuration Log	38
11	Transportation Receipt	39
12	Document Transaction Card	40

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

I. INTRODUCTION

This ADP System Security Plan describes the security measures in effect for Phase II 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 II network, residing within the AIPRL are: a "VAX Cluster" consisting of the VAX 11/750 (MDAC), VAX 11/785 (IDS-1), VAX 8650 (IDS-2) systems, two (2) Micro VAX (LWD,WPS) participating in the network, DECnet Product, and the APTEC-1 and APTEC-2 I/O computers (IOC'S).

The VAX 11/750 is a dedicated controller located in Room 2-1-1 with an attached MDA FIRE-240 film writer and terminal located in Room 2-1-8 (See Figure 1).

The VAX IDS-1 (VAX 11/785) is located in Room 2-1-2, with image display station and terminals located in Rooms 2-1-1, 2-1-2, 2-1-3, and 2-1-5 (See Figure 1).

The VAX IDS-2 (VAX 8650) is located in Room 2-1-5, with an image display station in Room 2-1-4, and terminals in Room 2-1-4 and 2-1-5 (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, and (b) VAX 11/750 (SL) located in Room 2-1-9 (See Figure 1).

The LWD Micro VAX is a dedicated controller for the LWD device located in Room 2-1-8 (See Figure 1).

All terminals not located within the TEMPEST enclosure are connected to the VAXcluster and MicroVax systems by way of TEMPEST-approved fiber-optic multiplexors to various locations within the SCIF. Data lines, in conduit, connect each remote terminal to the TEMPEST multiplexors (See Figure 2).

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

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 who reports directly to the Unit General Manager for Special Programs, (with dotted-line responsibility to the BIFSCO), is the Facility Security Representative (FSR) for Hawkeye Plant (See Figure 3). In addition to the ADPSSR and the FSR, Mr. Jonathan P. Hobbs and Mrs. Concetta E. Curatalo, have been named as the Computer Facility Security Officers (CFSO), to monitor the day-to-day security of the system.

(b)(3)

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 4). The TEMPEST enclosure was tested to NSA65-6 and recertified by Program B Message 3975 dated 30 October 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 II configuration for the two VAX nodes and associated peripherals operates in the Multi-Compartmented (for two or more NFIB members) as defined in Paragraph V.A.2, SCIREQ 84, dated August 1984.

~~WARNING~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

The Phase II 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 II 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.
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:

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- 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

~~-WARNING-~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

(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 II configuration is listed in Figure 5. The system configuration (functional diagram) is shown in Figure 6. The security features of the VAX systems are:

- a. Volatile memory (i.e., no residual memory exists when power to units is turned off). The VAX 8650 does have a battery back-up, to prevent loss of data during a power outage.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- b. Memory bounds mechanism which prohibits system users from reading/writing in memory occupied by the Operating System or other system users.
- c. The VAX instruction set includes both privileged and non-privileged instructions. Only privileged users, installed privileged images, or the operating system may invoke privileged instructions or use non-privileged instructions in a privileged context (i.e., access protected data). Non-privileged instructions are available to all users.
- 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 all nodes of the Phase II configuration is an unmodified VAX/VMS Release 4.5.
- 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.

~~WARNING~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- e. Maintains user accounts in a user authorization file which constitutes the basis for privilege and quota assignments.
- f. Maintains access control lists for additional and more flexible protection for files and devices. Used with file and system-wide security alarms, they allow for logging of successful and unsuccessful attempts to access files.
- g. Includes a break-in detection feature which allows terminals and/or user accounts to be disabled when a break-in attempt is detected. This capability is enabled with the SYSGEN parameters LGI_BRK_LIM set to 3, LGI_BRK_TERM set to 1, and LGI_BRK DISUSER set to 1.
- h. Utilizes a user identification code (UIC), on which the protection mechanism is based. The UIC is associated with each structure, file, volume, and device that the user owns. A protection mask is used to determine which UIC groups or members are allowed/denied access.
- i. 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 assures 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 previously been allocated to another file.

~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

High-water marking and erase features are enabled during volume initialization. The DCL command INITIALIZE/ERASE/HIGHWATER erases the entire volume and establishes highwater marking, erase on delete, and erase on extend features.

F. SYSTEM ACCESS CONTROLS

1. Each node in the Phase II configuration operates from a common system disk to ensure that the account and access control privileges do not differ among nodes. The authorization file (SYSUAF.DAT), rights database (RIGHTSLIST.DAT), and the network proxy authorization file (NETUAF.DAT) are maintained in the SYS\$COMMON:[SYSEXEC] directory. The establishment of access control lists, which are maintained as an integral part of each file, coupled with the three system files specified above, yields a capability comparable to that of VMSECURE.
2. Users are assigned to UIC groups based upon existing department and supervisory boundaries, and are assigned identifiers based upon access approvals and need-to-know criteria.

Each new account is assigned a username, default device and directory, UIC group, and appropriate resources quotas and limits. All other values for quotas, limits, and privileges are automatically copied from the DEFAULT user account. The GENPWD flag and the TMPMBX and NETMBX are established in the DEFAULT account.

Privileges other than TMPMBX and NETMBX are not granted to any users except system management and security accounts. System backups are performed through a captive, privileged account. The

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

SYSTEST and SYSTEST_CLIG accounts are disabled. The FIELD account is enabled as needed for maintenance by cleared personnel.

Applications requiring privileges are installed with the INSTALL utility after thorough scrutiny by systems and security administrators.

3. System logon passwords are randomly generated, English-like, and pronounceable words, six to eight characters in length.

Automatic password generation is provided by the DCL command SET PASSWORD and enforced by the AUTHORIZE command qualifier /FLAG=GENPWD.

Knowledge of system logon passwords is restricted to the individual receiving the password. Users must select one of the system-generated passwords from the list provided through the DCL command SET PASSWORD.

Appropriate system logon passwords will be changed whenever an actual or suspected system compromise occurs, or whenever a system user leaves the project. Otherwise, all system passwords are changed every six (6) months.

4. A user who exceeds a login failure limit of three (3) is automatically denied further access to the system and his/her account must be reactivated by the FSR. This feature is enabled with the SYSGEN parameters LGI_BRK_LIM set to 3 and LGI_BRK_DISUSER set to 1. VAX/VMS sets the DISUSER flag in the UAF record for the user account.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

5. ACL-based protection is applied to all rooted, project-level directories, granting access to holders of the appropriate project identifier and denying access to all others.

Each user is assigned a "home" directory in an organization-level root and one or more project-level roots determined by access approval and need-to-know criteria.

Organization-level roots are defined for UIC groups based upon existing departmental and supervisory boundaries. Each root is protected via the UIC-based protection mechanism, with the protection code specified as SYSTEM:RWE, OWNER:RWE, GROUP:RE, WORLD:E and with the owner declared as [group,*].

Project-level roots are defined for identifiers specifically declared for program compartmentation. Each root is protected via the ACL-based protection mechanism with the ACL specified as:

(IDENTIFIER=project identifier,ACCESS=EXECUTE)

(IDENTIFIER=[*,*],ACCESS=NONE)

The project identifier is declared as the owner of the root directory and, therefore, the directory; - cannot be changed by users. - perusal is not possible. - W:E results in "pass-through" capability.

User directories created in organization-level roots are protected with a code of SYSTEM:RWE, OWNER:RWE, GROUP, WORLD. This results in no GROUP and no WORLD access to the directory. The user is declared as the owner of the directory. UIC and ACL protection can be modified at the discretion of the owner.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

User directories created in project-level roots are protected with an ACL specified as:

(IDENTIFIER=user__identifier+project__identifier,ACCESS=READ+WRITE+EXECUTE)

(IDENTIFIER=project_identifier,ACCESS=EXECUTE)

(IDENTIFIER=[*,*],ACCESS=NONE)

This results in read, write, and pass through access to a specific user (identified by UIC) who has also been granted the project identifier; permits only pass through access to all other holders of the identifier; and, denies access to all non-holders. The project identifier is declared as the owner of the directory, thus preventing the assigned user from modifying the directory ACL (since the user does not have CONTROL access).

Files created under ACL protected directories have ACL automatically defined; granting CONTROL to the assigned user and denying access to all others. These ACLs may be modified at the discretion of the user, provided that other users have already been granted the project identifier. Ownership of all files remains with the project identifier.

Project ownership of directories and files is enforced by first, establishing project ownership of the directory root and second, granting approved users the project identifier with the RESOURCE attribute enabled.

Rooted directories are directories which appear to be the master file directory (MFD) for a logical disk volume. Sub-directories appear as top-level directories at the logical disk volume. (See Figure 7).

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

6. The NETUAF.DAT, SYSUAF.DAT, paging and swap files are protected through normal UIC-based protection, excluding any access by the WORLD.

All file access failures, for any reason, are logged on the system's hardcopy console and OPERATOR.LOG.

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 including unclassified 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.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- 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 by 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.

~~WARNING-~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

(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.



removable

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

and fixed drives have no customer-approved sanitization procedure to declassify disk media. Media may only be released to another similar SCI classified environment after execution of the ISSD-approved ERASE routine and upon written approval from the customer assigned ISSO and the appropriate program management office.

Fixed-media drives which become inoperable or which must be declassified will have the platters removed from the HDA for classified control and/or destruction.

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.

~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

1. Automated Audit Trail:

Automated audit trails are derived from the VMS accounting log data, with image-level accounting enabled, and access alarm messages for various system events. OPCOM messages recorded in OPERATOR.LOG and printed at the system's hardcopy console include: all unsuccessful file accesses; login and logout events from network, remote, interactive, batch, and detached resources; all changes to the system authorization file and rights database; volume mounts and dismounts; and execution of the SET AUDIT command.

Accounting activity is enabled automatically at system boot time with the SET ACCOUNTING/ENABLE command.

Security alarms are enabled automatically at system boot time with the SET AUDIT command.

Security messages are extracted from OPERATOR.LOG using the FILTER.COM procedure. These messages are written to microfiche and scrutinized daily by the Computer Facility Security Officer (CFSO). Any irregularities are reported to the FSR and the ADPSSR.

Accounting log data is reviewed periodically and examined for unusual resource utilization, unfamiliar usernames, unusual login times, and execution of specific systems programs.

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.

~~-WARNING-~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- b. Open/Close Log (Figure 8): Used to identify individuals who close/open the computing facility by date and time.
- c. Computer Center Security Checklist (Figure 9): 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 10): Used to identify all software available to the system.
- f. Transportation Receipt (Figure 11): 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 12): 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.

~~WARNING-~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

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

ADP system circuitry, cable housing, and power installations are installed according to specifications set forth in "Security Standards of Classified Plaintext Distribution in Contractor Installations" and "Special Conduit Systems for Overhead Distribution", as excerpted from Military Handbook 232.

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 3975, dated 30 October 1986.

V. ADP SYSTEM OPERATIONS

A. SYSTEM PREPARATION AND INITIALIZATION PROCEDURES

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

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

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

2. I/O devices and direct access storage devices not to be used during processing operations are taken off-line.
3. All demountable data and program storage media not to be used during classified processing are removed from the system and placed in approved storage containers.
4. The CPU's internal memory is sanitized by turning the keylock switch to the OFF position. The VAX-8600 requires that the time-of-year clock's battery backup be switched off which also supplies battery backup to memory.
5. All fixed media required during classified processing, including the dedicated system disk, are enabled by inserting the appropriate "select plug" into each drive and powering the drive up.

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 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.

~~WARNING~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

3. System terminals are configured automatically at boot time. All login sequences, both successful and unsuccessful are controlled by VMS and logged in the OPERATOR.LOG file and the ACCOUNTING.DAT file. All file accesses are controlled by the system with any unsuccessful attempts logged on the system's hardcopy console.
4. If a security-related, abnormal processing operation occurs involving any storage media (i.e., system compromise or data spillage), processing will be manually stopped and the ADP Systems Security Representative will be contacted for determination of action to be taken. System anomalies are investigated through interactive investigation of system audit and authorization files, such as: ACCOUNTING.DAT, SYSUAF.DAT, NETUAF.DAT, OPERATOR.LOG, NETSERVER.LOG, etc.
5. If processing is to continue, the system is initialized and re-booted with the dedicated version of the operating system.
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.

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

C. OUTPUT CLASSIFICATION/HANDLING PROCEDURES

System generated output produced by AIPRL is sorted and distributed by USERNAME. It is the user's responsibility to ensure that all material is properly classified and controlled. Any output not collected by the end of the day is secured in a approved storage container inside the TEMPEST. If the user has not claimed the output within two (2) days, it is destroyed in accordance with applicable customer directives.

It is the user's responsibility to ensure that printed material obtained via auxiliary printers (i.e., ancillary to distributed terminals) is properly classified, labeled, and controlled.

Host to PC/workstation data transfers via terminal emulation are permissible provided that object storage media is classified and controlled, commensurate with category and level of information to be transferred.

D. MODE TERMINATION

Upon completion of processing, the following actions are taken:

1. A shutdown routine is initiated to remove all users from the system and terminate all processing.
2. Operators remove all demountable data and program storage media from the system used during the classified processing period.
3. All fixed media enabled during classified processing, including the dedicated system disk, are disabled by removing the "select plug" from each drive and powering the drives down.

~~WARNING~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

4. The CPU's internal memory is sanitized by turning the keylock switch to the OFF position. The VAX-8600 requires that the time-of-year clock's battery backup be switched off which also supplies battery backup to memory.
5. Classified output such as printouts and magnetic tapes are handled according to customer approved procedures.
6. A removable, dedicated version of the operating system for unclassified processing is mounted and enabled for processing.

VI. SYSTEM MAINTENANCE

All system maintenance is performed by cleared personnel. Ancillary hardware is occasionally serviced by uncleared personnel according to the guidelines below.

- 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.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

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. As required, separate, dedicated copies of the operating system and diagnostics are 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.

~~WARNING~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

ADP system users are provided a special briefing concerning their responsibilities to prevent "write-down" of sensitive classified data, i.e., to a user's individual directory.

-WARNING-

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

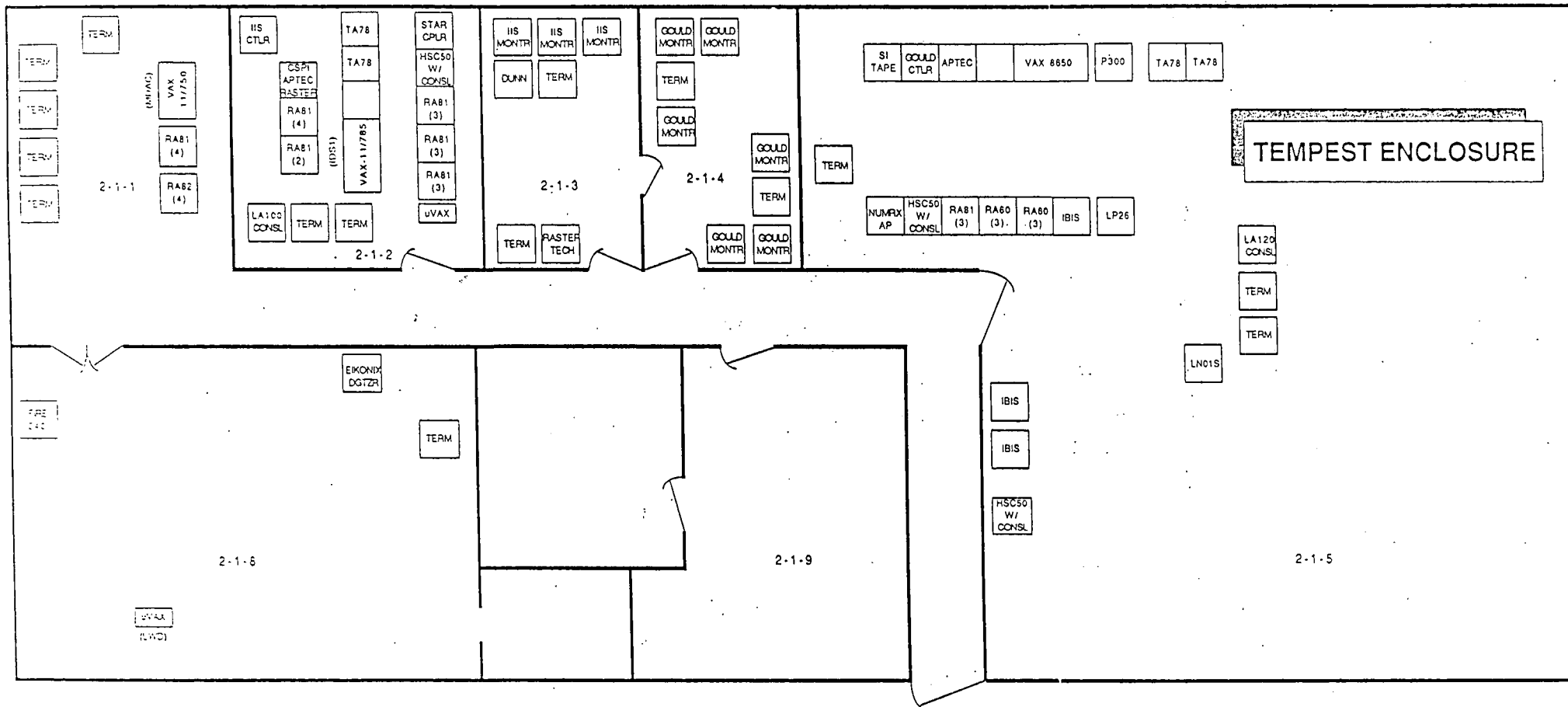


Figure 1. VAX Cluster Floor Plan

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

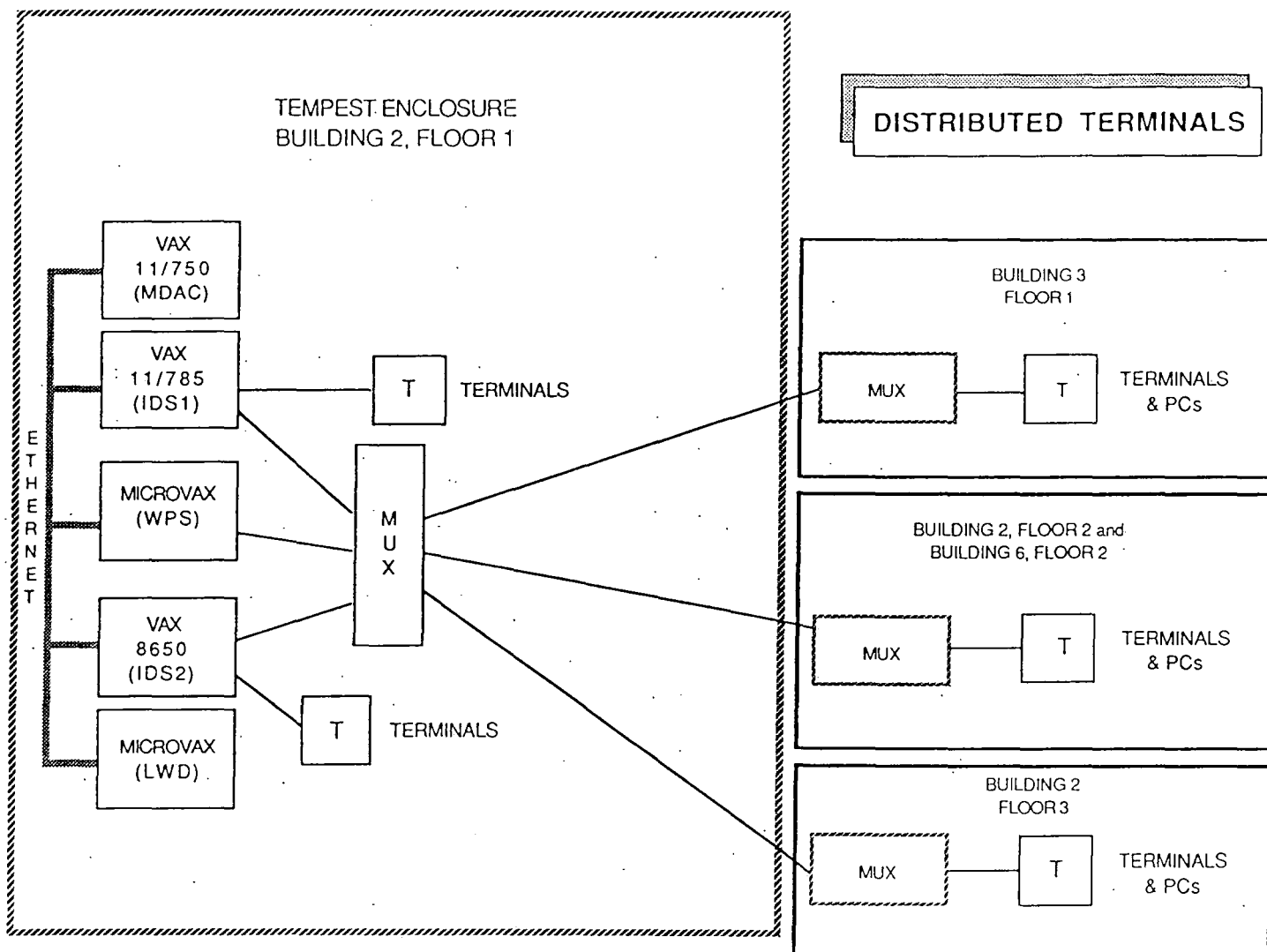


Figure 2. Distributed Terminal Connection

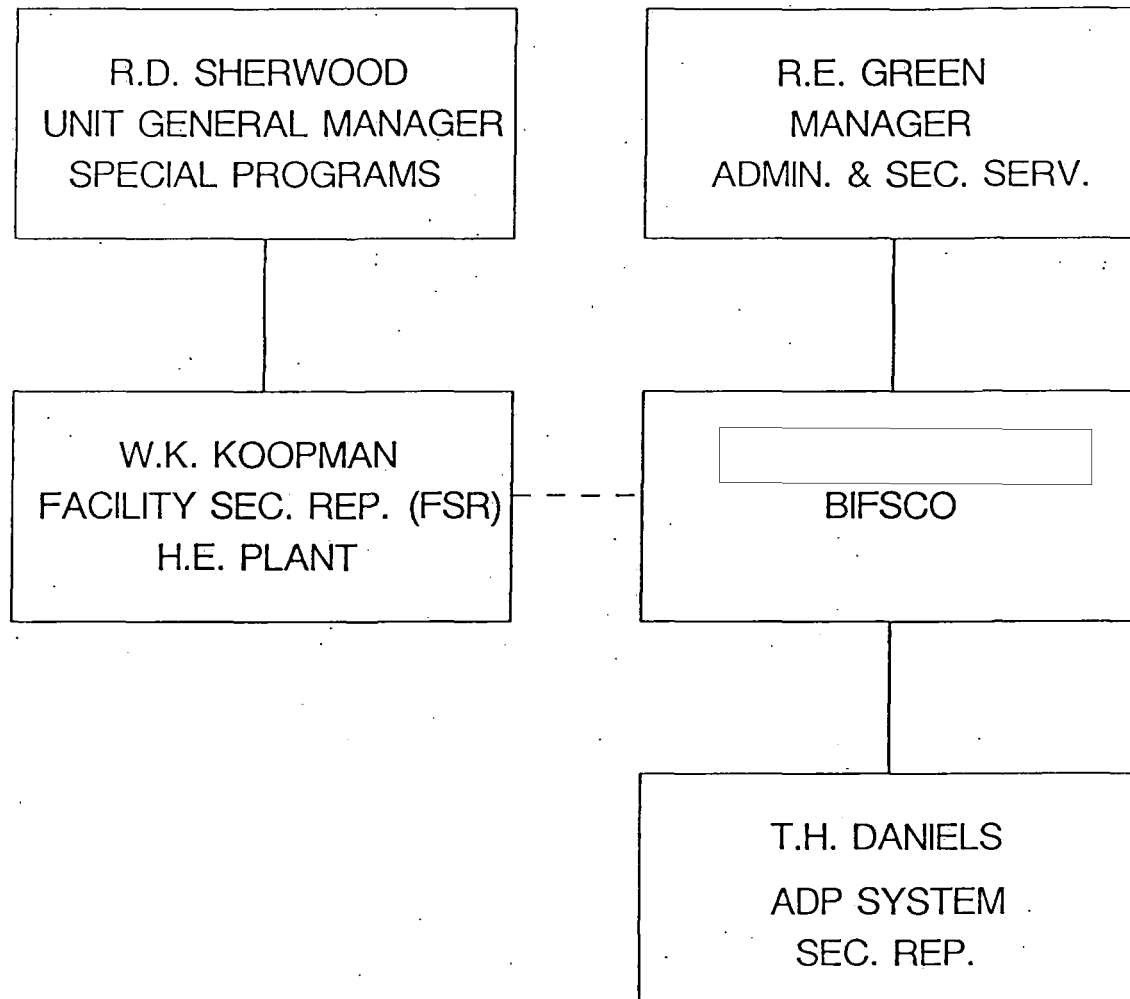
~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87



(b)(3)

Figure 3. ADP System Security Organization

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

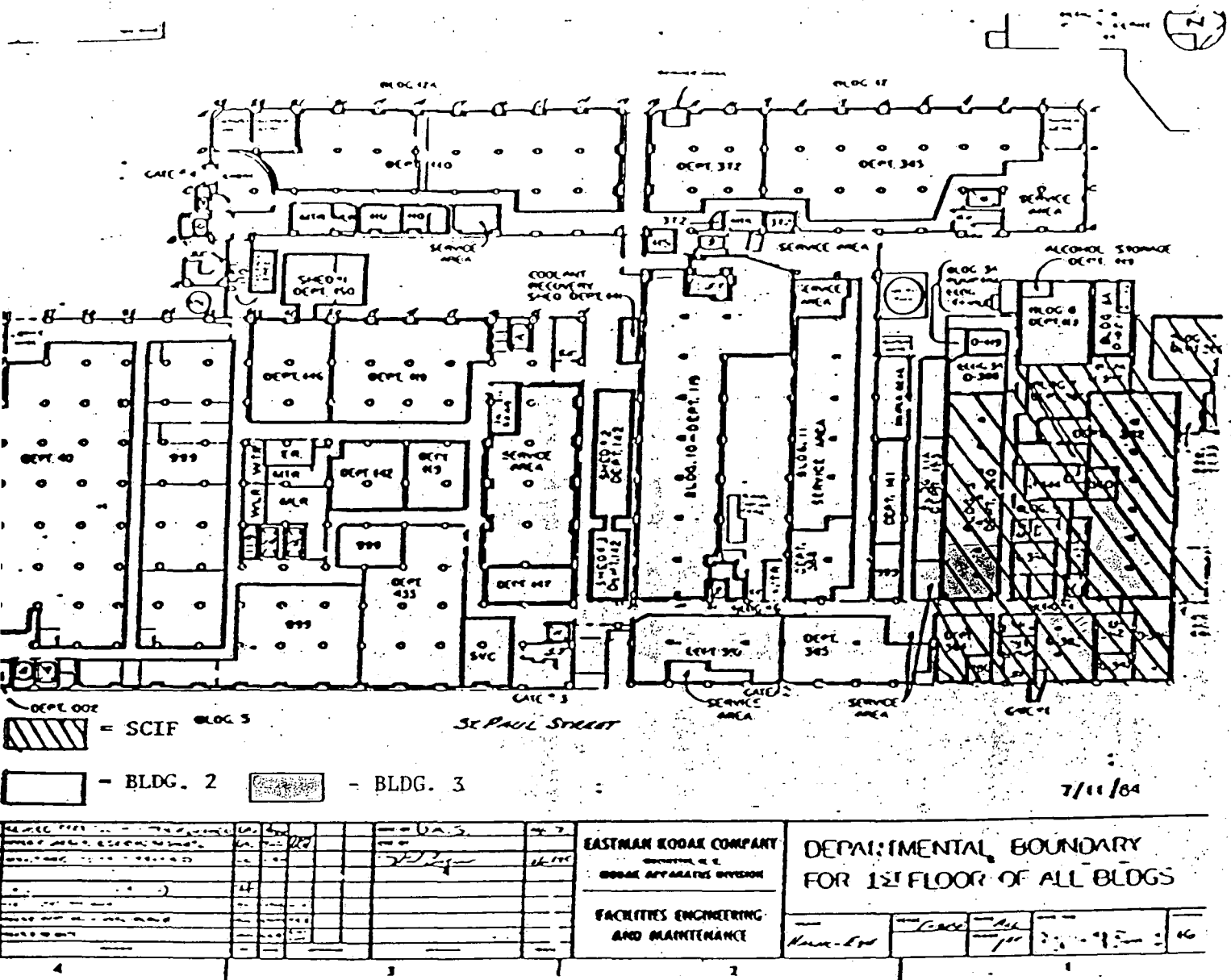


Figure 4. Hawk Eye Floor Plan

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

Qty	Model	Description
12	VT220	ASCII Terminal
1	VT102	ASCII Terminal
17	VT240	ASCII Terminal w/ graphics
1	LA120	8600 System Console
1	LA100	785 System Console
1	IIS-70	Image Processor
1	CSPI-MAP310	Array Processor
1	Numerix-432	Array Processor
3	IBIS 1400	Disk Drive
1	LP26	600 lpm Band Printer
1	P300	300 lpm Matrix Printer
1	LN01S	12 ppm Laser Printer
3	TA78	1600/6250 bpi Tape Drive
1	Tu78	1600/6250 bpi Tape Drive
1	RT 80	Raster Tech Display Driver
2	Aptec-IOC	Aptec 2400 I/O Computer
1	VAX-11/750	Computer
1	VAX-11/785	Computer
1	VAX-8650	Computer
15	TPC4	IBM Personal Computer
1	SC008	Star Coupler
3	HSC50	Disk/Tape Controller w/ LA12C console
18	RA81	Fixed Disk Drive
4	SA482	Fixed Disk Drive
6	RA60	Removable Disk Drive
1	SI-9700	1600/6250 Tape Drive
1	Gould IP8500	Gould Image Procesor
1	Eikonix 785	Digitizer
1	Fire 240	Laser Film Writer
1	Dunn 631	Camera System

Figure 5. System Hardware

~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

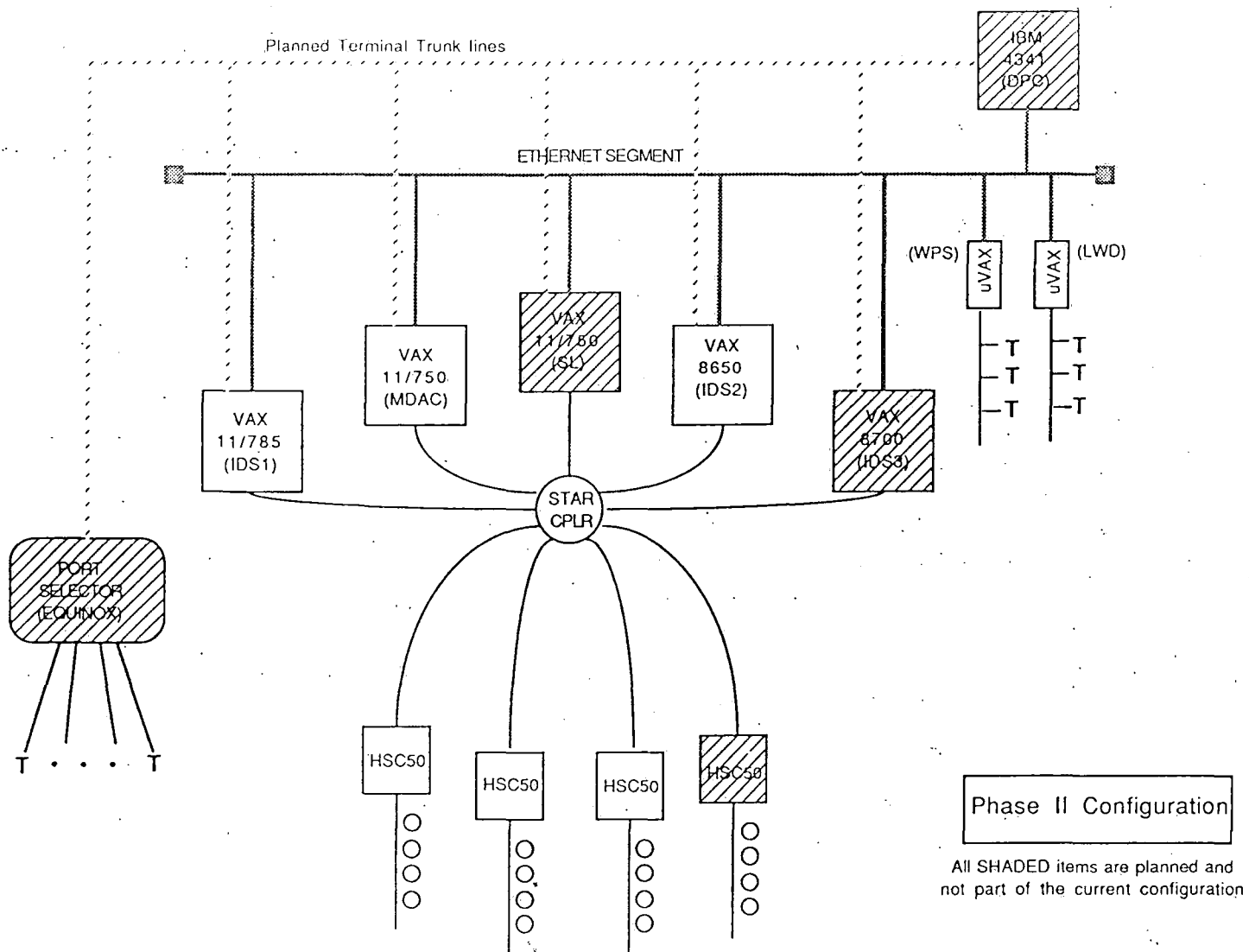


Figure 6. System Configuration

~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

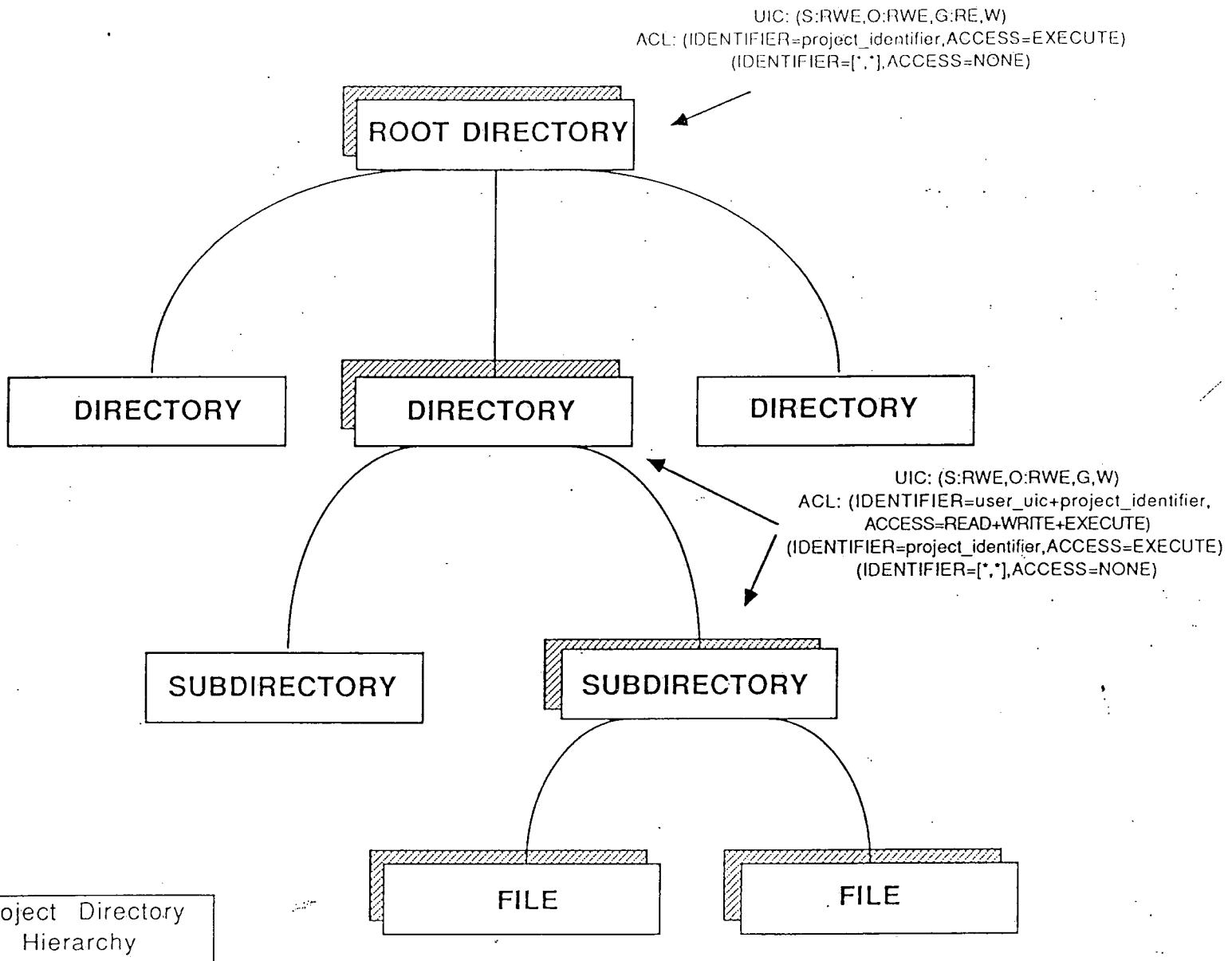


Figure 7. Project Directory Hierarchy

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

SECURITY CONTAINER RECORD SHEET																	
Month		Container No.		Location		Area		Plant									
TIME		TIME		CHECKER QUARD		Floor-bldg		TIME		TIME		CHECKER QUARD					
DATE	OPENED	BY	CLOSED	BY	TIME	BY	TIME	BY	DATE	OPENED	BY	CLOSED	BY	TIME	BY	TIME	BY
1									17								
2									18								
3									19								
4									20								
5									21								
6									22								
7									23								
8									24								
9									25								
10									26								
11									27								
12									28								
13									29								
14									30								
15									31								
16																	

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

61-3226 (11-77)

Figure 8. Open/Close Log

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

Preparation: Date Time Initials

- 1) Notify users that the system is shutting down for classified processing.
- 2) Clear all unauthorized personnel from the computer area.
- 3) Shut the system down with the SHUTDOWN procedure and HALT the CPU.
- 4) Sanitize the system
 - 4a) Turn the CPU off and leave for five (5) minutes.
 - 4b) 8650 only. Turn the time-of-year clock off and leave for five (5) minutes.
- 5) Disable all drives: a) spin down; b) remove plugs; and, c) power down.
- 6) Remove unclassified boot console media and secure.
- 7) Remove unclassified system pack and secure.
- 8) Enable all drives required for classified processing: a) power up; b) insert plugs; and, c) spin up.
- 9) Insert classified boot console media.
- 10) Boot the system at the console.

Processing: Date Time Initials /

- 11) Monitor system access at console.
- 12) If a security-related, abnormal processign operation occurs involving any storage media, stop processing and contact Tom Daniels, extension 32328.
- 13) If processing is to continue, reboot the system at the console.
- 14) Log all security-related abnormal system operations and security violations and report them to Tom Daniels, extension 32328.
- 15) 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 /

Figure 9. Computer Center Security Checklist

~~SECRET~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

- 16) Shut the system down with the SHUTDOWN procedure and HALT the CPU.
- 17) Sanitize the system
 - 17a) Turn the CPU off and leave for five (5) minutes.
 - 17b) 8650 only. Turn the time-of-year clock off and leave for five (5) minutes.
- 18) Disable all drives: a) spin down; b) remove plugs; and, c) power down.
- 19) Remove classified boot console media and secure.
- 20) Remove and secure all demountable data and program storage media and secure.
- 21) Place all classified waste, notes, listings, working papers, and printer ribbons requiring destruction in the specified burn container.
- 22) Mount and enable unclassified system pack.
- 23) Enable all drives required for unclassified processing:
 - a) power up; b) insert plugs; and, c) spin up.
- 24) Insert unclassified boot console media.
- 25) Boot the system at the console.

Figure 9. Computer Center Security Checklist (Cont'd)

~~—WARNING—~~

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

~~SECRET~~

HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

Vendor	Description
Digital	VAX/VMS v4.5
Digital	FORTTRAN 77 v4.2
Digital	CMS v2.0
Digital	MMS v2.0
Digital	OPS5 v1.0
Digital	ADE v2.4
Digital	FMS v2.2
Digital	C v2.0
Digital	LISP v1.0
Digital	Pascal v 3.2
Digital	SPM v3.0
ISSCO	DISSPLA v10.5
International Math & Statistics Library, Inc.	IMSL Math Library
Gould	LIPS Digital Image Processing Software v1.0
IIS	System 570 Image Processing Software
Raster Technologies	ONE/80 Software Library
CSPI	SNAP II Extended Arithmetic Function Library v 3.0
Penn. State University	Minitab v5.1.3
Aptec	Staple processor and driver routines
Numerix	Arex/Avid Fortran Development System

Figure 10. Software Configuration Log

~~WARNING~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

TRANSMITTAL RECEIPT

No.118002

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

Description of Contents: _____

Transmittal Authorized By: _____
(Signature) (Date)☐ Class.☐ Uncl.

Description of Package, Envelope, Etc.: _____

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

Signature Receipt(s) and Date(s):

1) _____ 4) _____

2) _____ 5) _____

3) _____ 6) _____

NE 3157 @ 74

LAST ENTRY SHOULD BE CROSS REFERENCED TO SUBSEQUENT CONTROL SYSTEM

Figure 11. Transportation Receipt

~~SECRET~~

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY

~~SECRET~~

BIF-008-WA-000047-OH-87

ORIG	DOC NO	TR	COPY	TO	FROM	O	M	VS
DCR				COPY				
<input type="checkbox"/> FIRST ISSUANCE <input type="checkbox"/> CURRENT CUSTODIAN (ENTER BELOW)				<input type="checkbox"/> DESTROY <input type="checkbox"/> TRANSFER TO PROGRAM FILE <input type="checkbox"/> NEW CUSTODIAN (ENTER BELOW)				
LAST NAME FIRST NAME INITIAL				TO LAST NAME FIRST NAME INITIAL LOCATION				
CUSTODIAN'S RECORD				REC'D (SIGNATURE) (DATE)				
LOCATION				INVENTORIED				
				WE CERTIFY THIS MATERIAL WAS				
				COMMITTED TO DESTRUCTION ON: (DATE)				
				(SIGNATURE) (SIGNATURE)				

DOCUMENT TRANSACTION CARD RE 2538 (5-69)

P40/4814

Figure 12. Document Transaction Card

-WARNING-

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

~~SECRET~~HANDLE VIA BYEMAN
CONTROL SYSTEM ONLY