(b)(3)

~~SECRET~~

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE
SUBJECT TO CRIMINAL SANCTIONS

BIF-008-WA-000034-OH-87-004
This document contains 36 pages
Copy 4 of 9 copies
Date 31 MARCH 1987

BIF008WA-000034OH/87 4 U

# SECURITY PLAN

FOR

IBM-4341

DATA PROCESSING CENTER

(DPC)

T. H. Daniels
ADPSSR

for R. D. Sherwood
R. D. Sherwood
Unit 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 the Data Processing Center (DPC), a component of the Advanced Image Processing and Recording Laboratory (AIPRL) located on the entire First (ground) Floor of Building 2, at the Eastman Kodak Company, Hawkeye Plant, 20 Avenue E, Rochester, NY 14650. The DPC, IN CONJUNCTION WITH THE OTHER COMPONENTS OF AIPRL, supports investigations of current and future digital image systems and provides secure facilities to process NRO sponsored multi-program Sensitive Compartmented Information (SCI), up to and including, Top Secret BYEMAN and TK. AIPRL was approved to process multi-program SCI by program B message 9152, dated 13 May 1982.

## 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 1). 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. SECURITY ENVIRONMENT

The DPC is located in Room 2-1-5 within the Hawkeye Plant. This room, measuring 38' by 46', is in a portion of the Tempest enclosure on the Ground Floor in the north quadrant of a Customer-approved SCIF and the east portion of the AIPRL, Building 2, (see Figure 2). The TEMPEST enclosure was retested to NSA 65-6 specifications and recertified by Program B message 3975, dated 30 October

1986. The DPC was approved for "Open" shelf storage by Program B message 4026, dated 10 June 1983.

## IV. SYSTEM SECURITY

### A. MODE OF OPERATION

1. The DPC IBM 4341 computing facility and all associated peripherals, including the remote terminals (Room 3-1-5), operate in the MULTI-COMPARTMENTED MODE as defined in Paragraph V.A.4., Page 13, SCIREQ84, dated August 1984.

2. Security measures commensurate with processing TOP SECRET BYEMAN and SI/TK information as well as the appropriate SCI control channels all in effect during all processing operations.

3. The DPC is currently more than 90% dedicated to processing for Program B and less than 10% dedicated to processing for Program A. In addition, a very small effort is dedicated to processing the the DMA. This processing, in total, supports three different customers and 12 different contracts. These contracts are processed concurrently.

4. The DPC system provides for unclassified, program-related software development activity, as approved by the cognizant Information Systems Security Officer (ISSO).

### B. PERSONNEL ACCESS CONTROLS

1. Personnel requiring unescorted access to the DPC and the associated terminal room (Room 3-1-5) are security approved according to DCID 1/14 standards and access approved for individual SCI

programs, as appropriate. The list of Customer-approved personnel authorize access to the DPC and the associated terminal room (currently 90) is maintained by the Hawkeye Plant FSR.

2. Need-to-know is established by the appropriate EK Project Manager, and must be confirmed by an appropriate indicator on the individual's secure area badge. (Also see Paragraph IV.C.2.)

3. There are at lest two Customer-approved persons in the DPC at all times, unless the DPC is properly secured by the S&G safemaster extension 50 locking device.

4. There are at least two Customer-approved persons in the remote terminal room at all times during processing operations.

5. Two persons are required to open and close the AIPRL, the DPC, and the remote terminal room.

6. Entry to and normal egress from AIPRL is via the main entrance to the TEMPEST enclosure, controlled by an electronic cypher unit.

7. Access to the DPC is via a simplex lock installed at the entrance door.

8. Requests for official escorted visits to the AIPRL, DPC, and the associated terminal room must be approved on a case-by-case basis by the FSR as directed by the Contracting Officers Security Representative (COSR), and the following actions are taken:

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

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

c. An "Uncleared Visitor in Area" sign is placed on the door of the DPC.

d. A flashing colored light is placed in the corridor outside the DPC.

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

f. The 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. The Hawkeye Plant SCIF was approved by the cognizant COSR.

b. Normal entry to and egress from the SCIF is provided by only one entrance, i.e., 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. DPC:

a. Normal entry to and egress from the DPC entrance is controlled by a simplex lock unit. For downtime purposes, the DPC entrance is also secured with an S&G safemaster extension 50 locking device.

4. Alarms:

a. The DPC 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 DPC.

c. All alarms are connected to the Wells Fargo annunciator system located at the 24 hour guard post.

D. SYSTEM HARDWARE

1. The DPC system hardware, all non-TEMPEST equipment, is listed in Figure 3. The system functional configuration is shown in Figure 4, and the remote terminal functional configuration is shown in Figure 5.

2. Connection from the DPC to the remote terminals, located in Room 3-1-5, is as follows: the IBM 3274 Terminal Controller, located in Room 2-1-5, connects to a TEMPESTED multiplexor (MUX) via coaxial lines. Connection from the TEMPESTED MUX to the TEMPESTED MUX located in the remote terminal room (Room 3-1-5) is via fiber optic lines (in conduit). Coaxial lines connect the TEMPESTED MUX located in Room 3-1-5 to the remote terminals (see Figure 6).

3. The ten fixed disk storage units associated with the DPC system (1 ea IBM 3350-A2F unit, 3 ea IBM 3350-B2F units, the 2 IBM 3380-AA4 units, and the 4 ea IBM 3380-B04 units) were Customer-approved for "Open" storage by Program B message 4026, dated 10 June 1983.

4. The IBM 4341 Processing Unit internal memory is classified non-volatile. The Customer-approved sanitization routine used is described in Paragraph IV.G.4.d, following.

5. Magnetic tape is used for all backup (archival) operations. Each project is written to a separate pool of magnetic tapes.

6. The Kodak KOMSTAR is a micro image processor used to produce 4" or 5" microfiche for program listings and security-related system audit reports.

E. SYSTEM SOFTWARE

1. The operating system used for this computing facility is an unmodified IBM VM/SP release 4. Figure 7 lists all DPC software, IBM and non-IBM.

2. The VM/SP operating system:

   a. Runs in a privileged mode.

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

   c. Handles all input/output functions related to available and shared resources.

   d. Provides an audit trail record (see paragraph IV.H.)

3. The VM/SP operating system has two components, a Control Program (CP) and a Conversational Monitor System (CMS).

   a. The CP manages the resources of a single real processor to provide for using virtual machines.

   b. Each CP command has one or more privilege classes assigned.

   c. The CMS provides a wide range of user-dialog and time-sharing services so that files can be created/managed/compiled and problem programs tested/run.

4. The VM/SP operating system provides for the creation of a virtual machine for each system user based on information stored in the VM/SP directory. The entry for each system user includes:

   a. Virtual I/O Device

   b. Privilege Class(es)

c. Accounting Data

d. Virtual Storage Size

e. Dispatching Priority

f. Optional Virtual machine Characteristics

5. Additionally, the VM/SP operating system provides for the assignment of one or more privilege class(es) to each system user so that each user can be restricted to precisely what the user needs to perform an assigned function (JOB).

6. VMSECURE version 2.1, a security software package, with the Rules Facility and password encryption capability is installed and used by the DPC system.

F. SYSTEM ACCESS CONTROLS

1. Prior to being allowed access to the system, each user is identified as Customer-approved and possessing an established need-to-know for data associated with either a specific SCI program or a set of SCI programs.

System passwords are individual user unique pronounceable identifiers, no less than six (6) and no longer than eight (8) characters in length. System passwords are exclusively provided by the Facility Security Representative (FSR), Walter K. Koopman, and one alternate individual specifically designated by the FSR.

Knowledge of system passwords is restricted to the individual receiving the password and the FSR. System passwords are changed every six (6) months, but will also be changed whenever an actual or suspected system compromise occurs, or when either the FSR or his designated alternate leaves the project.

2. Users are assigned to groups based on existing department and supervisory boundaries.

3. Each new account is assigned a username, security group, a virtual machine and a 191 minidisk.

4. Implementation of the NOLOG option, for an SCI virtual machine, limits all users to linking to that virtual machine, but prohibits them from logging onto that virtual machine.

5. 191 minidisks which house data for a specific compartment (SCI) may be shared only by users who have access approval for that specific SCI compartment.

6. Each project resides on a separate physical volume.

7. VMSECURE security software package, with the Rules Facility in REJECT mode, provides exclusive user access at the minidisk level to data residing on direct access devices which are online to the system. To access any information in the system, rules must be, and are, specifically written on user, group, or system level.

8. The VMSECURE security software package, with the Rules Facility implemented, performs the following functions:

a. Denies access by default, i.e., no rule, no access.

b. Dynamically creates rules to disable the user on excessive invalid logons. Maximum invalid logons are set at three (3) for the DPC. The user's logon must be reactivated by the Computer Facility Security Officer (CFSO) when the user is forced off the system because of exceeding this maximum limit.

c. Maintains rules at three (3) levels, System, Group, User. Further, these rules are implemented in that hierarchy. When rules are written to allow links to other than the owner of the minidisk, the conditional access approach is used, by adding the LOGPASS option to the rule. This approach eliminates establishing minidisk passwords. The user requesting the link to another user's minidisk must supply his own logon password before he is allowed access to the requesting link, providing there is a rule allowing the access.

d. Coordinates directory maintenance and rules modification by removing rules for userids that are deleted from the directory and changing rule references when the userid changes.

e. Provides history information about successful and unsuccessful access attempts.

9. Access to specific projects are controlled by rules written, based upon the FSR's recommendation, indicating access approval for each user of each project.

10. Alpha-numeric "Slave" printers are not authorized and are not used in the DPC or remote terminal area.

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 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 channel(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 Customer-approved receipting method is used to ensure that accountability is maintained (see Paragraph IV.G.3 immediately below).

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 the 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 TD290343, magnetic tape degausser; the label identifying the assigned document control number as well as the highest security classification and SCI control channel(s) of the information ever recorded on them is not removed.

2. High energy magnetic tapes (i.e., magnetic tapes having a coercivity of 325 oersteds or more) are not authorized and are not used.

3. 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 (i.e., inoperable), 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 unuseable, they are destroyed in accordance with applicable Customer directives.

d. Internal Memory:

A Customer-approved IBM supplied software routine is used to sanitize internal memory of the IBM 4341 mainframe. Sanitization is accomplished by setting zeros in all data bit locations and verifying the overwrite process. Malfunctions which prevent the successful operation of this routine will be immediately reported to the assigned Customer ISSO.

e. Minidisks:

New minidisks are defined and formatted by issuing the VMSECURE MANAGE command. This command automatically for-

mats the disk space, erasing all files and data on the minidisks, adds the space to the pool of available (unallocated disk space) and removes any existing directory links to the minidisk.

f. VMBATCH Subsystem:

The batch machine's 191 minidisk is erased before each job is started and after each job ends, thus data residing there will not be available to subsequent users of the machine.

The batch machine's virtual card reader is cleared before and after each job. Where possible, reader, punch, and print spool files are transferred to the custody of the job owner's virtual machine.

H. AUDIT TRAILS

The audit trail record capability implemented for the DPC system to protect Customer information is comprehensive and uses both automated and manual techniques.

1. Automated Audit Trail

a. The data used to produce automated audit reports are collected via the implementation of VMSECURE and VMSCHEDULE.

b. VMSECURE monitors and logs activity of the six (6) CP commands, i.e., AUTOLOG, LINK, LOGON, TAG, TRANSFER, and SPOOL. VMSECURE also logs all directory maintenance activity for all directory changes.

c. VMSCHEDULE, using the CLEAN EXEC procedure, coordinates the daily renewal of the VMSECURE AUDIT File; it extracts the AUDIT file for the previous 24 hour period, generates a report file, and produces (using the KOMSTAR equipment) a microfiche report for review and archiving. The Computer Facility Security Officer (CFSO) reviews this report daily, and reports irregularities to the FSR and ADPSSR.

2. Manual Audit Trail

The following manual audit trail records are reviewed by the CFSO, FSR, and ADPSSR, at a minimum, once each week.

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 8):
Used to identify individuals who close/open the computing facility by date and time.

c. 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.

d. Software Configuration Control Log:
Used to identify all software available to the system.

e. 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.

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

I. DOCUMENTATION

1. 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 DPC.

J. STORAGE AREAS

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

K. COMMUNICATIONS LINKS

1. 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

1. The TEMPEST enclosure is constructed and approved per NSA-65-6 specifications, and received TEMPEST certification from the Customer's Communications Security (COMSEC) authority via Program B message 3975, dated 30 October 1986.

M. SYSTEM OUTPUT

1. The DPC system utilizes the Customer-approved and provided VM "CLASSIFY" command to force proper assignment of a security classification level for system generated output.

2. System generated output produced by the DPC is sorted and distributed by USERID. 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 secured in a approved storage container inside the DPC. If the user has not claimed the output within two (2) days, it is destroyed in accordance with applicable customer directives.

## V. ADP SYSTEM OPERATION

NOTE: System startup occurs only on Monday morning and system shutdown occurs only at the end of the week, either Friday evening or sometime on Saturday, whichever prevails.

A. SYSTEM PREPARATION

Prior to processing Customer information, normally each Monday morning, the following actions are completed by the on-duty DPC personnel.

1. Confirm that only authorized personnel are present in the DPC.

2. Confirm that the TEMPEST fire door and the DPC external and internal doors are unlocked and closed.

3. Confirm that all demountable magnetic storage media not required for the intended processing are removed from the system and properly secured.

4. Power on the GANDALF cabinet to provide control for the terminals.

5. Power ON the system.

6. Execute the Customer-approved CPU internal memory sanitization routine.

7. IPL the system.

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 and the appropriate SCI.

2. During normal hours, a minimum of two (2) security approved individual are present in the computing facility. 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. All successful and unsuccessful access attempts are controlled and audited by VMSECURE, and recorded in the VMSECURE AUDIT File.

4. If a security-related, abnormal processing operation occurs involving any storage media (i.e., system compromise of data spillage), processing will be stopped and the ADP Systems Security Representative will be contracted for determination of action to be taken. System anomalies are investigated through investigation of the VMSECURE AUDIT file.

5. If processing is to continue, the system is restarted using a reserved and 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 of 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 possible.

C. MODE TERMINATION

When required:

1. Secure remote terminal area.

2. Clear system printer buffers.

3. Remove any demountable magnetic media and secure in approved storage.

4. Execute the Customer-approved CPU internal memory sanitization routine.

5. Power OFF the system.

6. Power OFF the GANDALF cabinet.

7. Secure all safes.

8. Secure interior and exterior perimeter TEMPEST doors.

9. Secure the Building No. 2 fire door.

VI. SYSTEM MAINTENANCE

The Eastman Kodak policy is to use Customer-approved Maintenance personnel whenever possible. When not possible, the following procedures apply:

A. All 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 DPC 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 or diagnostics are maintained within the DPC component and stored and controlled as though classified. Maintenance representatives are not allowed to remove any magnetic media from the DPC.

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

G. Malfunctioning circuit boards having nonvolatile memory components may be released from the DPC 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 DPC component, the name of the individual, the name of the assigned escort, specific maintenance performed, and the date and time are recorded in the log.

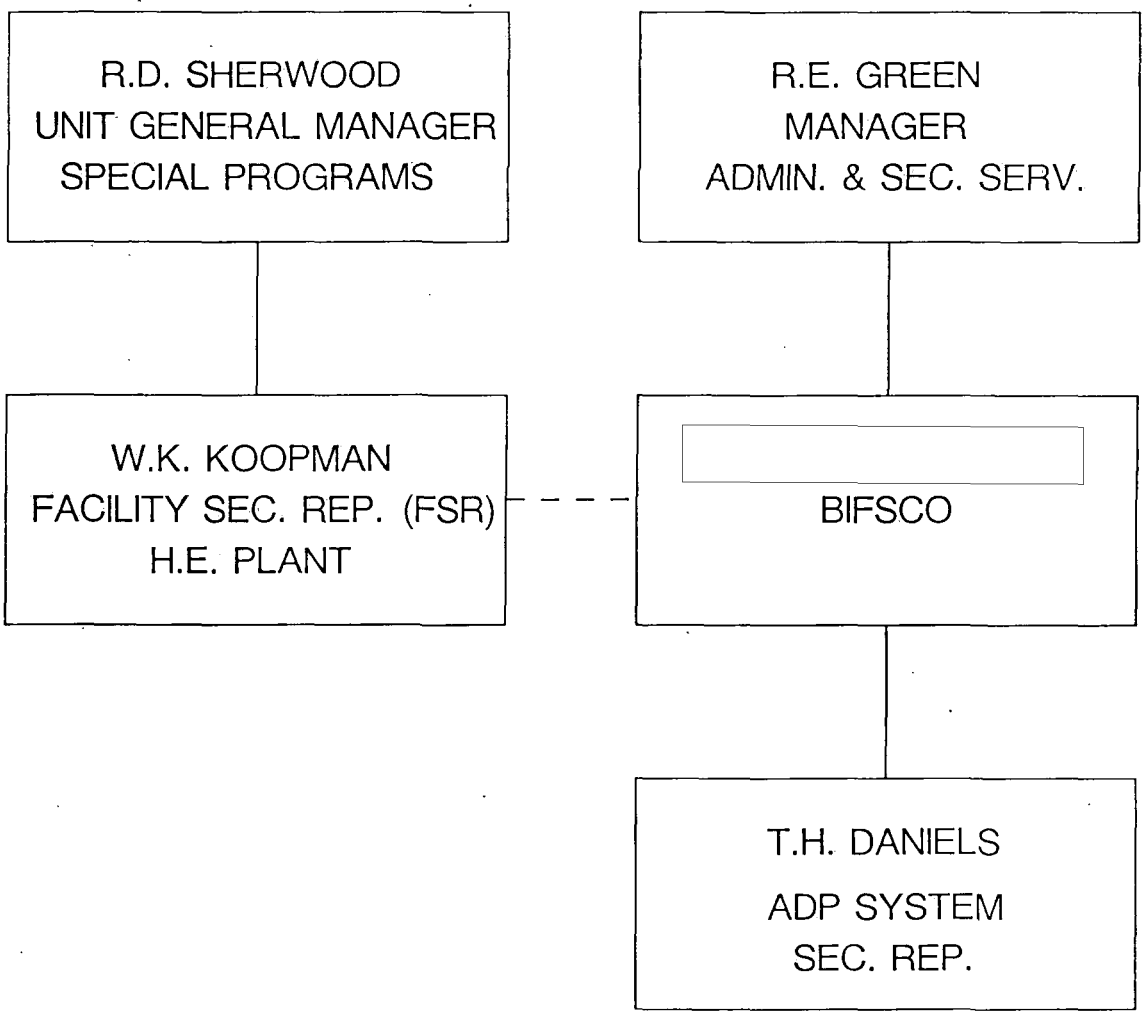
I. Remote diagnostics are not utilized for maintenance purposes for the DPC component. Approval from the Customer's ISSO will be requested in advance should the use of remote diagnostic links come under consideration.

VII. SECURITY EDUCATION

All Eastman Kodak Company personnel who work in the SCIF 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 System Security Representative before access to the DPC is granted.

DPC 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 minidisk or temporary disk.

ADP SYSTEM SECURITY ORGANIZATION




(b)(3)

Figure 1. ADP System Security Organization

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

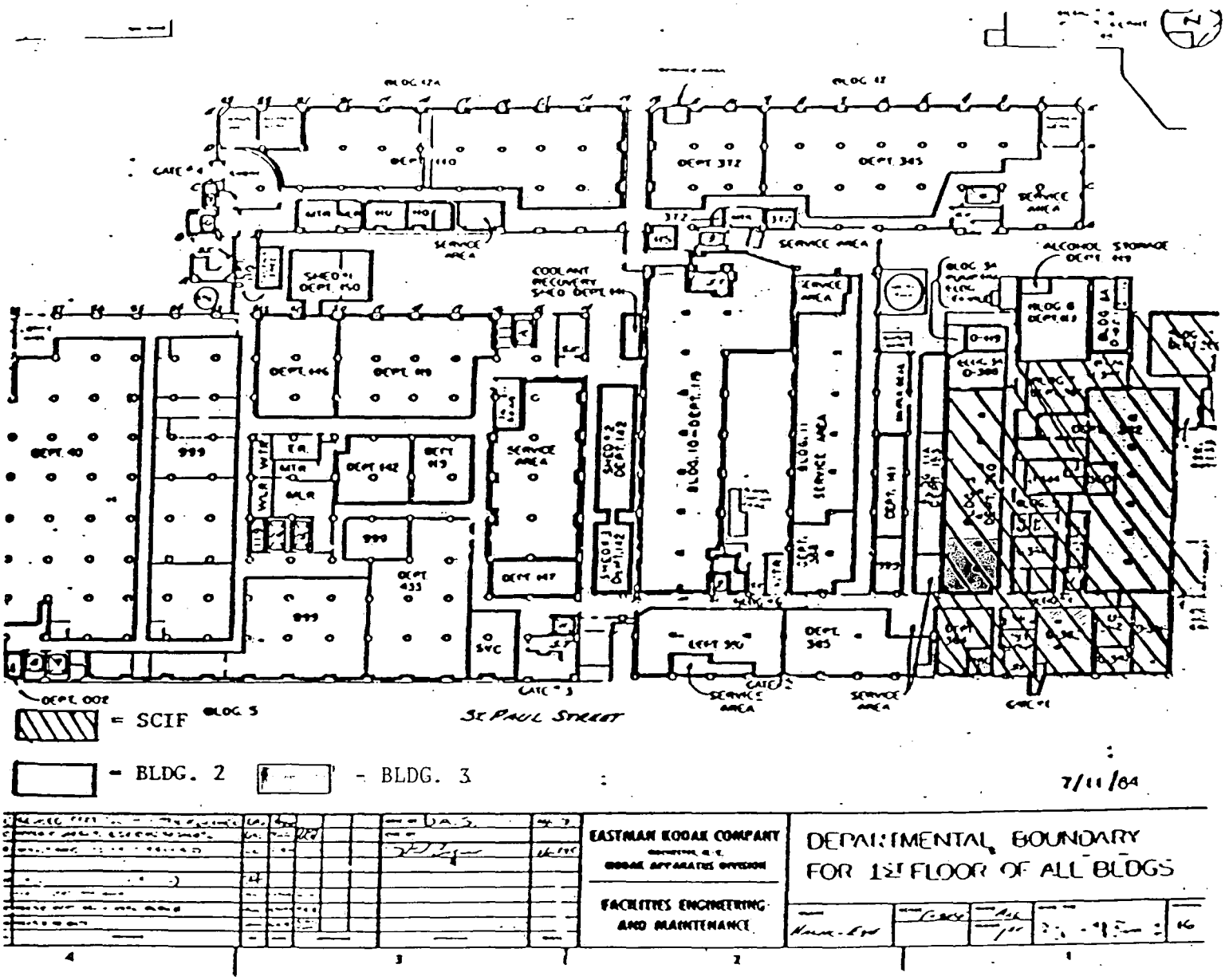



Figure 2. HE First Floor Plan

-WARNING-

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

DPC (Room 2-1-5)

| | QTY | MODEL NO. | SERIAL NO. | DESCRIPTION |
|---|---|---|---|---|
| IBM | | | | |
| | 1 | 4341-P12 | 12213 | CPU (16.0 MB) |
| | 1 | 3278-2A | 4C721 | CPU CONSOLE |
| | 1 | 3268-002 | 14095 | CPU PRINTER |
| | 1 | 3880-003 | 44686 | DISK CONTROLLER |
| | 1 | 3880-001 | 11095 | DISK CONTROLLER |
| | 2 | 3380-AA4 | 20605 20657 | DISK (AA4) |
| | 4 | 3380-B04 | 50753 52512 | DISK (B04) |
| | | | 51829 53626 | |
| | 1 | 3350-A2F | 25425 | DISK (A2F) |
| | 3 | 3350-B2F | 90487 91305 73907 | DISK (B2F) |
| | 1 | 3803-002 | 20736 | TAPE CONTROLLER |
| | 4 | 3420-6 | 57535 T0310 | TAPE UNIT (MOD-6) |
| | | | K2782 K2784 | |
| | 2 | 3420-8 | M9284 M9285 | TAPE UNIT (MOD-8) |
| | 1 | 3274-D31 | 60825 | TERMINAL CONTROLLER |
| | 4 | 3278-002 | E3400 E7212 | TERMINAL (B&W) |
| | | | D5284 5T757 | |
| | 2 | 3279-3B | 65057 55866 | TERMINAL (COLOR) |
| | 1 | 3279-3X | C5084 | TERMINAL (COLOR) |
| | 1 | 2821-001 | 18192 | PRINTER/READER CONTROLLER |
| | 1 | 1403-N01 | 33015 | PRINTER |
| | 1 | 2540-001 | 10932 | CARD READER |
| | 1 | 3203-5 | 22691 | PRINTER |
| | 1 | 3705-E08 | 42110 | COMMUNICATION CONTROLLER |
| | 1 | 3287-2C | C9255 | PRINTER |
| NON-IBM | | | | |
| | 1 | 1039 | 2677 | CALCOMP PLOTTER |
| | 1 | 921 | 2241 | CALCOMP CONTROL UNIT |
| | 1 | 300 | 950 | KODAK KOMSTAR |
| | 1 | 7550A | 2520A29629 | HP GRAPHIC PLOTTER |

REMOTE TERMINAL ROOM (3-1-5)

| | QTY | MODEL NO. | SERIAL NO. | DESCRIPTION |
|---|---|---|---|---|
| IBM | | | | |
| | 8 | 3279-3B | 24361 24362 44910 | TERMINAL (COLOR) |
| | | | 44911 55560 55814 | |
| | | | 55865 55867 | |
| | 2 | 3279-3X | C5082 C5086 | TERMINAL (COLOR) |

Figure 3. DPC System Hardware

**-WARNING-**

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

# ROOM 2-1-5

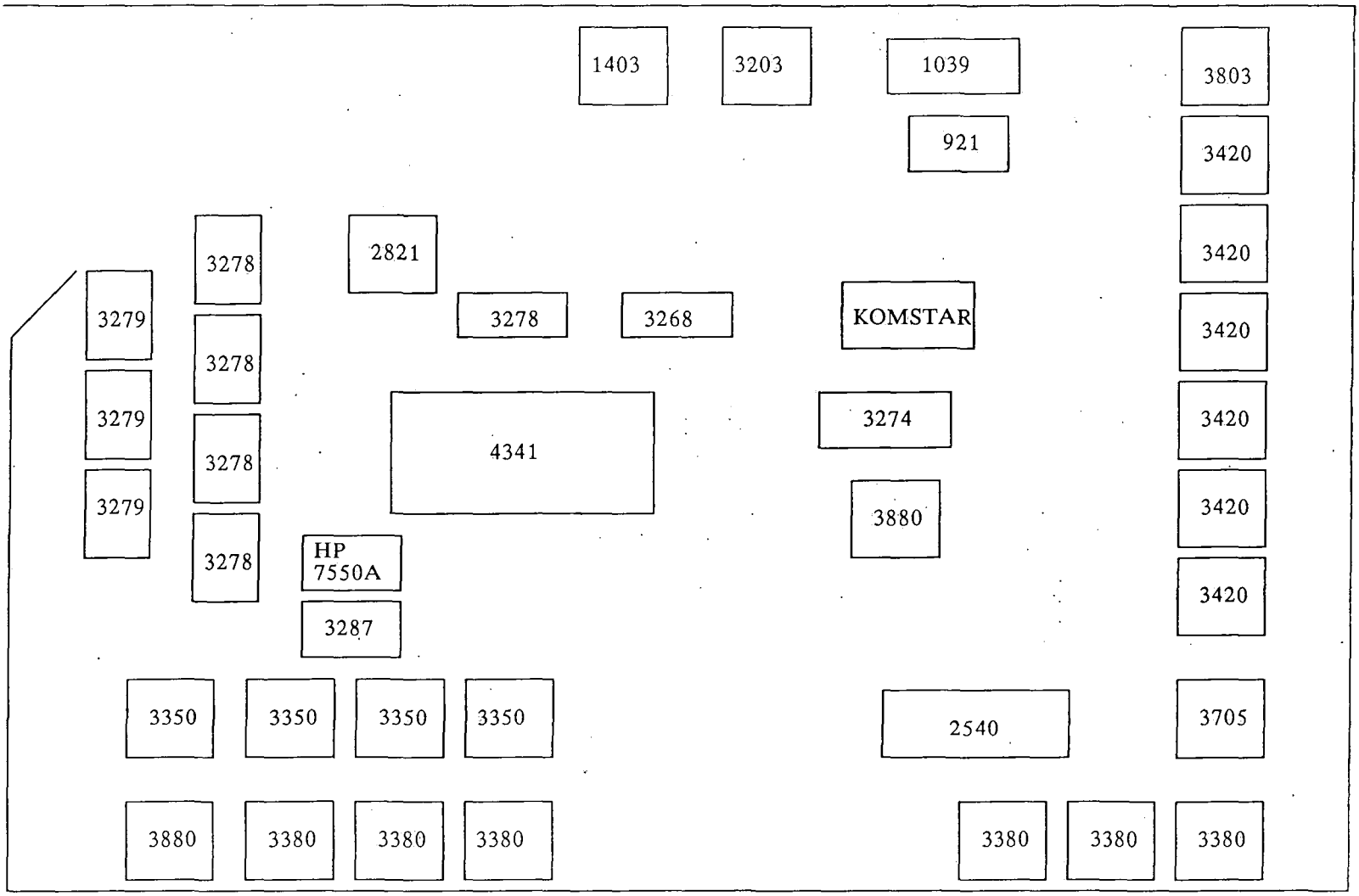



Figure 4. DPC System Configuration

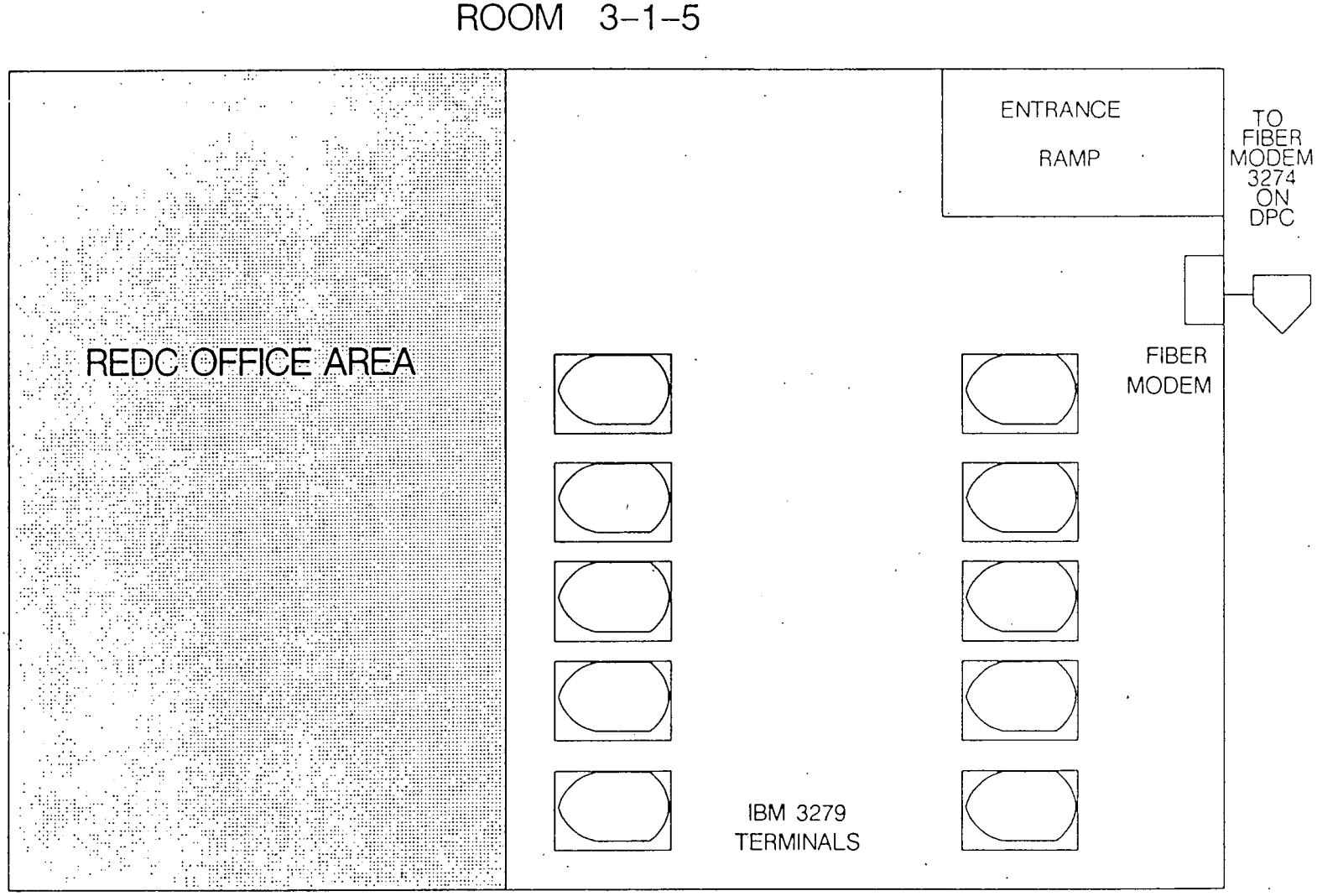



Figure 5. Remote Terminal Room

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

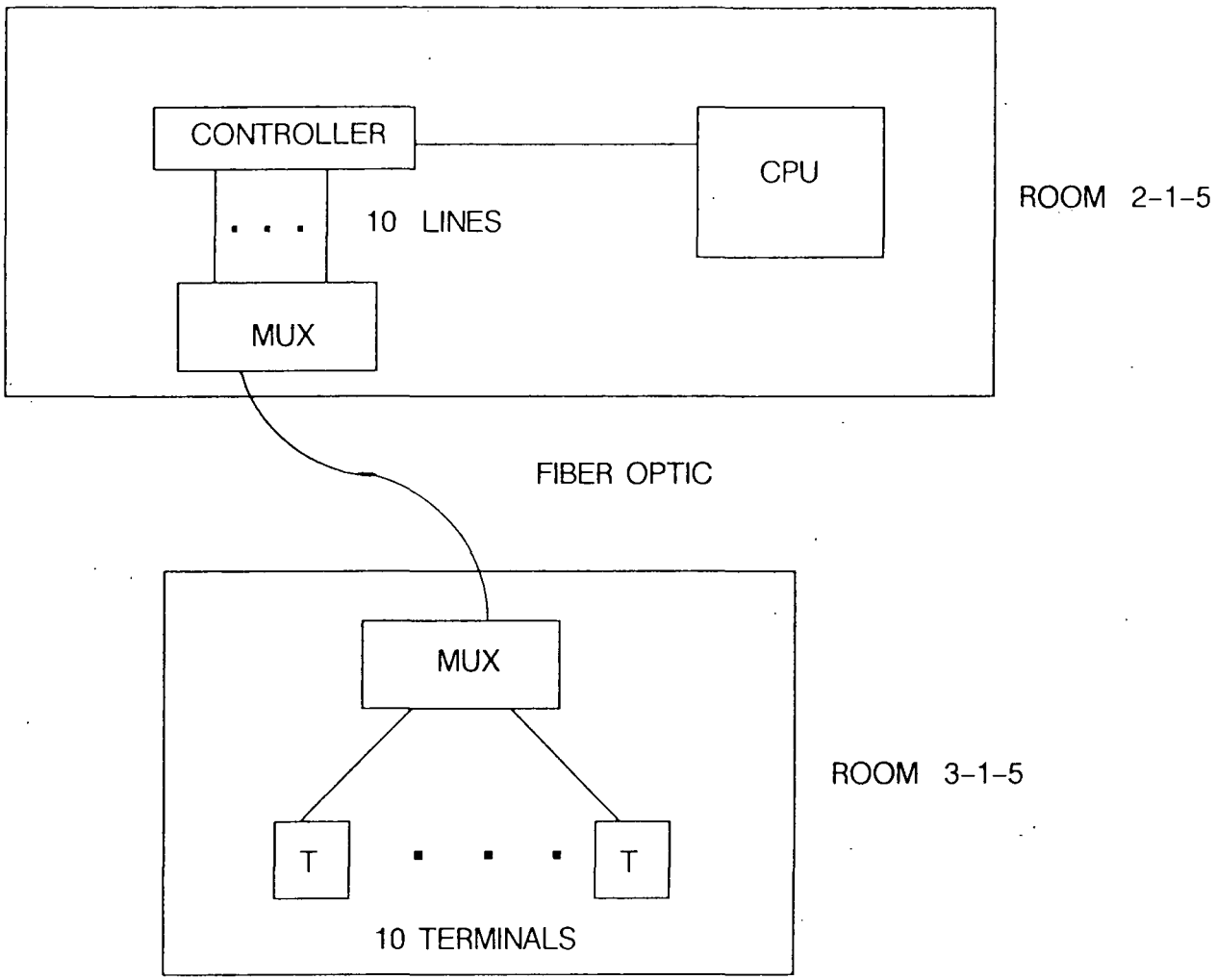



Figure 6. DPC/Terminal Room Connection

IBM SOFTWARE

VM/SP RELEASE 4

ACF/NCP
ACF/SSP
ACRITH SUBROUTINE LIBRARY
CMS VIRTUAL SPOOL READER DISPLAY
ELEMENTARY MATH LIBRARY
EMULATION PROGRAM
EREP
E/S PRODUCTIVITY FACILITY
FORTRAN UTILITIES FOR VM/370
GRAPHICAL DATA DISPLAY MANAGER
INFORMATION SYSTEMS - VM/SP
INTERACTIVE PRODUCTIVITY FACILITY
ISPF/PDF VM/SP, VM/CMS
OS PL/I OPTIMIZING COMPILER LIBRARY
PASCAL/VS COMPILER
VM BATCH SUBSYSTEM
VM MONITOR ANALYSIS PROGRAM
VS FORTRAN COMPILER AND LIBRARY
VS FORTRAN INTERACTIVE DEBUG
VSE/VSAM

NON-IBM SOFTWARE PRODUCTS

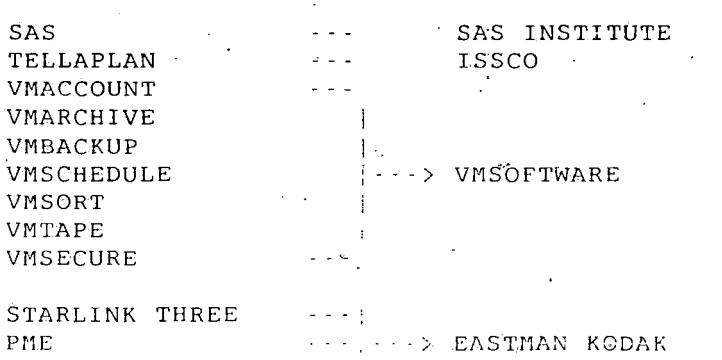



Figure 7. DPC System Software

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

SECURITY CONTAINER RECORD SHEET

Month _____ Container No. _____ Location _____ Area _____ Plant _____
(floor-bldg.)

| DATE | OPENED TIME | BY | CLOSED TIME | BY | CHECKED BY GUARD | CHECKED TIME BY GUARD |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |
| 12 | | | | | | |
| 13 | | | | | | |
| 14 | | | | | | |
| 15 | | | | | | |
| 16 | | | | | | |

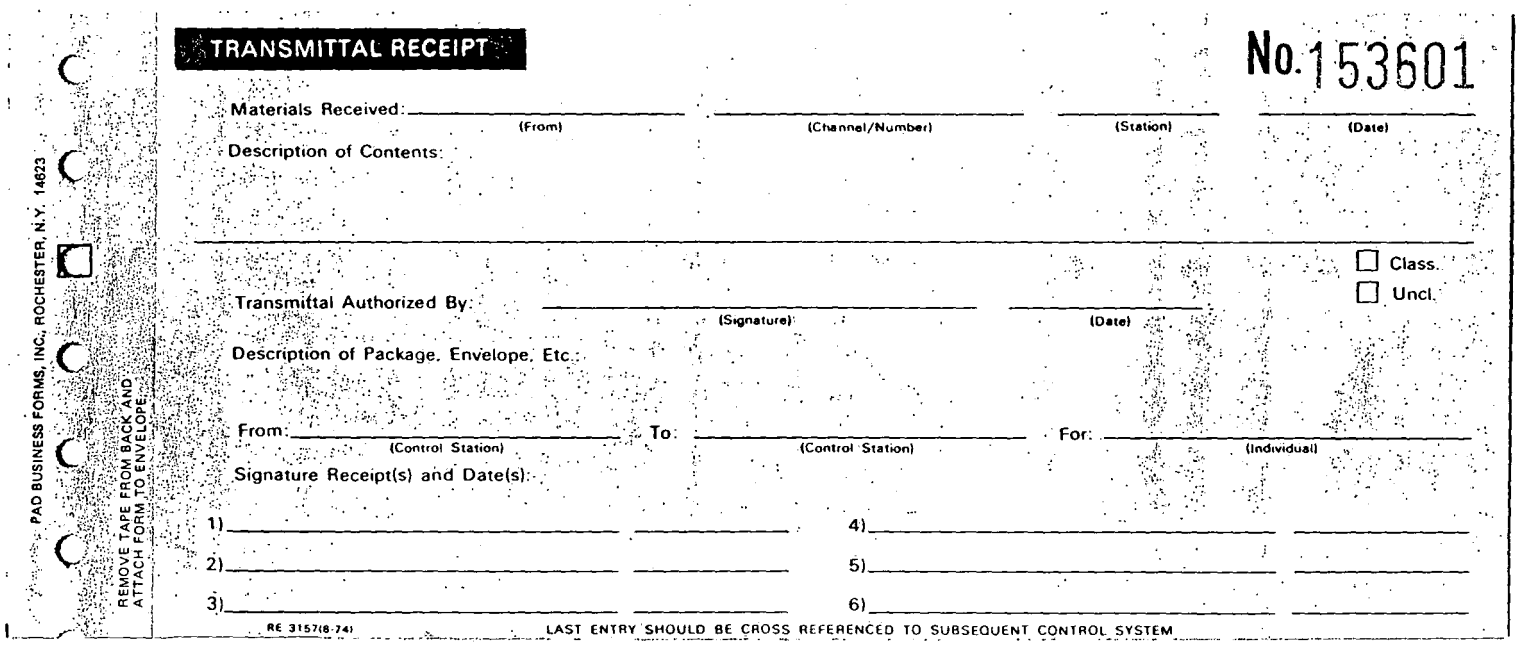
| DATE | OPENED TIME | BY | CLOSED TIME | BY | CHECKED BY GUARD | CHECKED TIME BY GUARD |
|---|---|---|---|---|---|---|
| 17 | | | | | | |
| 18 | | | | | | |
| 19 | | | | | | |
| 20 | | | | | | |
| 21 | | | | | | |
| 22 | | | | | | |
| 23 | | | | | | |
| 24 | | | | | | |
| 25 | | | | | | |
| 26 | | | | | | |
| 27 | | | | | | |
| 28 | | | | | | |
| 29 | | | | | | |
| 30 | | | | | | |
| 31 | | | | | | |

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

Figure 8. Open/Close Log

-WARNING-

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



TRANSMITTAL RECEIPT

No. 153601

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

PAD BUSINESS FORMS, INC., ROCHESTER, N.Y. 14623

REMOVE TAPE FROM BACK AND ATTACH FORM TO ENVELOPE

Figure 9. Transportation Receipt

-WARNING-

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

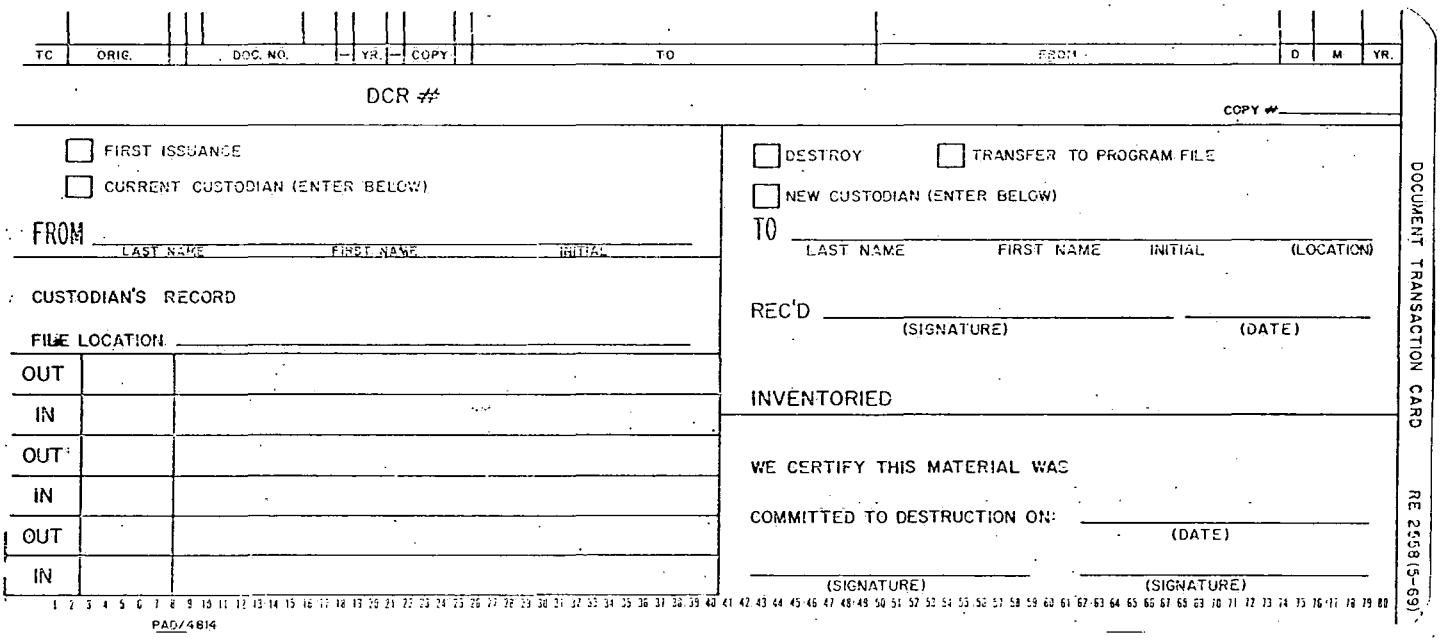



Figure 10. Document Transaction Card

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