Texas Department of Human Resources | Office for Information Systems

PHYSICAL SECURITY PROCEDURES

DATA CENTER

FOUNTAIN PARK PLAZA III

APRIL 1978

stems Processing Bureau

STATE OF TEXAS

DEPARTMENT OF HUMAN RESOURCES

PHYSICAL SECURITY PROCEDURES

DATA CENTER

FOUNTAIN PARK PLAZA III

Prepared by:

SYSTEMS PROCESSING BUREAU

April, 1978

PHYSICAL SECURITY PROCEDURES, DATA CENTER, FPP III

Record of Revisions

Revision#	Date of Revision	Pages/Attachments/Changes	Revised by (Initials)
1	June 19, 1978	Pages: TC-1, 3.1, 3.2, 3.3, 4.2, 4.6, 4.8, 6.1, 8.5, 9.2, & 9.4. Attachments: J, K-page 1, L-1, L-2, & R. Changes: On pages 4.7 & 7.4.	
2	June 22, 1978	Change: In Attachment D	
3	July 10, 1978	Page: 9.2. Change: On page 8.7.	
4	September 15, 1978	Attachments: J and Q.	
5	November 6, 1978	Pages: 3.2, 3.3, 4.2, 4.3, & 8.6. Attachment: J.	
6	January 6, 1979	Pages: TC-1, 1.1, 2.3, 3.3, 4.2, 4.3.1, 4.4, 4.5, 7.2, 7.4, 8.2, 9.2, & 9.2.1 Attachments: E, J, & L. Changes: To pages 1.1, 1.2, & 1.3.	
7	March 19, 1979	Pages: RR-1, 1.2, 1.3, 1.4, 4.3, 4.3.1, 4.4, 4.7, 4.8, 8.1, 8.2 & 9.2 Attachments: A, K-1, K-2, K-3, K-4, L, Q, & S.	

TABLE OF CONTENTS

Section 1. General

A. Policy

1. In order to accomplish the required Texas Department of Human Resources mission and provide the highest degree of security, access to the Data Center is carefully restricted to Department employees and specifically approved other persons whose duties and responsibilities require continuous or recurring access to the Data Center. These Department employees and other persons will be issued a Data Center Security Badge appropriately coded for the necessary level of access.

2. Persons who are not issued a Data Center Security Badge may be admitted to the Data Center under restrictive conditions only to accomplish official Department business as follows:

   a. Department employees or service personnel may be admitted when cleared by selected persons authorized to admit visitors.

   b. Other persons may be admitted only when cleared by Department employees occupying these managerial positions:

      1) Deputy Commissioner for Information Systems

      2) Chief, Systems Processing Bureau

      3) Assistant Chief, Systems Processing Bureau

      4) Administrator, Systems Production Division

      5) Director, Data Center

3. In the event that it is necessary for a bureau chief to request access for any person who is an employee of the federal government, an employee of the State government other than this Department, or any other person, that bureau chief should make advance arrangements with a Department employee occupying managerial positions shown above, in Section 1.A.2.b.1) - 5). In addition, the bureau chief making the request, or a designated representative of that bureau chief, must accompany persons in these categories while in the Data Center.

4. Persons who are elected officials, or employees of the Governor's office or Lieutenant Governor's office, may be admitted to the Data Center on specific authorization of the Deputy Commissioner for Information Systems or a person acting in the Deputy Commissioner's absence.

5. At all times access to the computer operational area is restricted to persons who have real and legitimate need for such access. Access is granted pursuant to the provisions of these Physical Security Procedures.

6. At such time that physical access to the Data Center and data terminals is not essential for effective Department operations, the appropriate administrator or other manager will assure that the Data Center Security Badge is withdrawn and access to the data terminals is restricted. In addition, where applicable, the user identification/password will be removed from the operating systems.

B. Purpose

The purpose of these procedures is to document methods for maintaining physical security of the Fountain Park Plaza III Building (FPP III), 2800 South Interstate Highway 35, Austin, Texas 78704. Methods for protecting FPP III, and the persons, equipment and other contents in it include:

1. Controlling access;

2. Utilizing fire prevention and other safety techniques; and

3. Establishing procedures for responding to emergency conditions.

C. Enforcement

1. Employee Responsibility

Each employee is expected to read, understand, and comply with, these procedures.

2. Supervisory and Managerial Responsibility

Supervisors and managers are expected to take continuing, affirmative measures to ensure that their employees know and comply with these procedures.

3. Penalties for Non-Compliance

a. For failure to comply with these Physical Security Procedures, personnel actions may be taken pursuant to the following sections of the Department Personnel Handbook:

4700 - Work Rules and Standards of Behavior and Performance

4800 - Recommendations for Adverse Personnel Action Against Employees

b. The Administrator, Systems Production Division, may deny authority to enter the Data Center to any individual who fails to comply with these procedures or who, in the Administrator's opinion, may otherwise constitute a security risk.

4. Authority of the Police Officer

The "Police Officer" was previously referred to as the "Security Guard". All references to "Security Guard" in these procedures are considered "Police Officer".

a. The Police Officer is an armed member of the Capitol Security Police force and is a commissioned peace officer of the State of Texas.

b. The Police Officer is charged with assisting in overall security of the Data Center/FPP III.

c. The authority of the Police Officer includes:

1) Protection of life and limb of persons

2) Arrest of persons

3) Search of the clothing of persons, as well as brief cases, packages, and other containers

4) Investigation and report of unusual activities or incidents in FPP III, and vehicle and equipment accidents on the premises

D. Responsibilities of Office for Information Systems (OIS) Organizations

1. Systems Development Bureau: Overall building management and coordination for FPP III and its surrounding grounds.

2. Systems Processing Bureau: Management control and coordination for;

a. Security of the Department's data processing services

b. Physical security of the Data Center/FPP III

c. These Physical Security Procedures including plans, policy development, publication, distribtuion and revision

d. Providing copies of the Physical Security Procedures and revisions to the Systems and Procedures Bureau for incorporaton, in summary, in the Department Administrative Management Handbook

e. Monitoring, testing and evaluating established security procedures and systems

f. Developing and coordinating contingency plans for the Data Center

3. Systems Production Division, as an operating unit of the Systems Processing Bureau, will accomplish tasks for operation and administration of the physical security systems in the Data Center, by:

a. Assuring compliance with these Physical Security Procedures

b. Conducting on-going use of the following systems:

1) Data Center Security Badge access

2) Fire prevention and detection

3) Door monitoring

4) Water detection

5) Moisture detection

c. Reporting to the Bureau Chief incidents of actual and suspected security violations of these Physical Security Procedures with statements of corrective actions as appropriate. These reports may be either written or oral and may include copies of activity summaries, personal injury reports, vehicle accident reports, FPP III evacuations for fire or other emergencies, malfunctions of systems stated in Section 1.D.3.b above, and any other matter that may be of management and staff physical security interest.

E. Revision of Procedures

1. Revision of these Physical Security Procedures may be made as follows:

a. Recommendation for revision may be made by any:

1) OIS organization supervisor

2) Holder of a Data Center Security Badge

3) Person employed in FPP III

4) Police Officer or the Chief, Captiol Security Police force

b. Recommendations may be written or oral.

c. Recommendations should be submitted in writing to the Chief, Systems Processing Bureau or orally to the staff member for security coordination in the Systems Processing Bureau.

d. Recommendations should include a brief description of the problem or potential problem with reasons for proposed change.

2. The staff of Systems Processing Bureau will analyze the recommendation, and, when it is deemed to have merit, will put the proposal into draft format and circulate it among appropriate persons and staff organizations.

3. On coordination and approval, the Chief, Systems Processing Bureau, will take action to have a revision published.

4. After publication of the revision, or rejection of the recommendation, the Chief, Systems Processing Bureau, will ensure that the person or staff organization originally submitting the recommendation for revision will be advised of the action taken.

Section 2. General Procedures for Access

A. Regular Work Hours

1. Fountain Park Plaza III

   FPP III may be entered or exited by the south door (St. Edward's Drive) or the east door (IH 35 frontage road) during regular work hours.

2. Data Center

   a. The Data Center is the one-story portion of FPP III northward from the double glass doors in the east lobby.

   b. A Data Center Security Badge (Section 4) or one of the authorized non-permanent badges described in these procedures is required for entrance. Persons admitted to the Data Center are required to wear the appropriate badge on the front clothing above the waist so that it is clearly visible. Data Center Security Badges must be worn with the photograph and color strip displayed.

   c. Persons may visit the Data Center if cleared to enter and signed in (see exception in Section 2.A.2.e.) by a person authorized to admit visitors (Section 3.D) on the Log of Visitors, DHR Form 9125 (Attachment A), and issued a non-permanent type badge for admittance (Section 4.H. and 5).

   d. On departing FPP III, persons who have previously signed in on the Log of Visitors will sign out, noting time of departure.

   e. Employees whose names appear on the Temporary Access List (Section 3.D) may be admitted to the Data Center on regular work days 6:45 A.M. - 6:00 P.M., without being signed in by a person listed on the Visitor Authorization List (Section 2.E). These employees are required to sign in on the Log of Visitors showing Temporary Access List as the authority.

B. Other Than Regular Work Hours

1. South Door Locked

   After 6:00 P.M. each regular work day, the Security Guard will lock the south door of FPP III. It will remain locked during non-regular work hours, through holidays and weekends and until 6:45 A.M. the next following regular work day. When the south door is locked, the east door must be used to enter and exit FPP III.

2. Security Guard Not at East Door

   On occasion the Security Guard will have to be away from the security desk at the east door for a few minutes. When this occurs at other than regular work hours, the Security Guard will follow the procedures

in Section 9.G. Anyone wishing to enter or exit the building while the east door is locked should wait at the east door for the return of the Security Guard.

3. Personal Identification Required

To ensure that only authorized persons are permitted access during other than regular work hours, the Security Guard may require each employee to provide proof of identification by comparing the picture on the employee's Department of Human Resources Identification Card, the Data Center Security Badge or other positive identification with the person seeking access.

4. Data Center

a. All persons admitted to the Data Center are required to wear the appropriate badge on the front clothing above the waist so that it is clearly visible. Data Center Security Badges must be worn with the photograph and color strip displayed.

b. Employees in possession of a properly issued Data Center Security Badge (Section 4.A) may enter the Data Center:

1) At any time that the badge is valid by using the badge in the Badge reader for each entry into the Data Center. These employees will not sign in.

2) At times other than when badge is valid by being signed in by a person authorized to admit visitors on the Log of Visitors, DHR Form 9125 (Attachment A), (Section 3.D, 4.H. and 5).

3) On exiting the Data Center, each person who has previously signed in on the Log of Visitors will sign out, noting the time of departure.

c. Persons may visit the Data Center if cleared to enter and signed in by a person authorized to admit visitors (Section 3.D.) on the Log of Visitors, DHR Form 9125 (Attachment A), and issued a non-permanent type badge for admittance (Section 4.H and 5).

d. Special clearance procedures are required for access to specified areas of the Data Center as follows:

1) Computer room (#199) and production control room (#195), as prescribed in Section 5, and when cleared by the computer room shift supervisor.

2) Documentation Center (#171), as prescribed in Section 4.I.3.

5. FPP III

a. Employees whose names appear on access lists (Section 3.A-C) may enter the southward two-story portion as follows:

1) If they regularly work in that portion of FPP III.

2) If they are issued a valid Data Center Security Badge.

3) If authority to enter is so stated on the access list.

b. Employees are required to sign in on the Building Register, DHR Form 9126 (Attachment b). On exiting FPP III, each person who has previously signed in on the Building Register will sign out, noting the time of departure.

c. Employees who regularly work in the southward two-story portion may authorize a visitor by the following actions:

1) Sign in the visitor by entering the name of the visitor and the time in the remarks column of the Building Register.

2) Be fully responsible for the conduct and actions of the visitor.

3) Ensure that the visitor departs FPP III prior to, or a the time of, the employee's departure.

4) Enter the time of the visitor's departure to the right of the visitor's name.

d. Special authorization and approval is required for persons, other than regular employees of FPP III who are not otherwise authorized by these procedures, to enter or remain in FPP III, after 5:00 P.M. or before 7:30 A.M., on regular day work hours, or anytime on weekends or holidays. The division administrator, or bureau chief responsible for the work of such persons should forward a request in writing to the Administrator, Systems Production Division. Such a request implies responsibility of the division administrator or bureau chief making the request for actions of the employees, who are not regular employees of FPP III, while they are in FPP III.

1) If the Administrator, Systems Production Division, approves the request, the division administrator or bureau chief making the request will be informed.

2) If the Administrator, Systems Production Division, does not approve the request, the division administrator or bureau chief making the request will be so notified with the reasons stated.

3) If the Administrator, Systems Production Division, does not approve the request, and the division administrator or bureau chief making the request believes that the request is necessary and appropriate, the matter may be referred to the Chief, Systems Processing Bureau, for resolution.

Either the Administrator, Systems Production Division, or the Chief, Systems Processing Bureau, approving a request, will provide written authorization of such approval to the Security Guard. The Security Guard will use only such authorization to admit persons to, or allow persons to remain in, FPP III.

Section 3. Maintenance of Access Lists

A. Access to FPP III and the Data Center

1. FPP III, the two-story south portion of the building, is open for entry during regular duty hours. During times other than regular duty hours, the building is restricted to persons on business with the Department, after proper identification and sign-in, as specified in these Procedures.

2. Access to the Data Center at all times is restricted to persons on business with the Department and in possession of an individualized Data Center Security Badge or otherwise properly admitted, pursuant to these Procedures.

B. Access List for Two-Story Portion of FPP III

1. Use

This list contains the names of persons who are authorized to enter the two-story portion of the building after regular work hours. It is used to clear persons for such entry (Section 2.B.2). It does not include the names of employees who hold Security Badges, since the Security Guard may clear these persons by referring to the Access List to the Data Center.

2. Additions and Deletions

Division administrators and bureau chiefs are responsible for currency and correctness of the access list to the two-story portion of FPP III as it relates to their employees. The Administrator, Systems Production Division, will circulate a copy of this access list to the Chiefs of the Systems Processing Bureau, the Systems Development Bureau, and the Systems Planning and Control Bureau for necessary revision approximately each calendar quarter. These lists should be promptly annotated and returned with current information. On receipt of the updated information, the Administrator, Systems Production Division, will update this list in the manual of the Security Guard.

3. Form

Access lists will be maintained for FPP III and the Data Center, for employee access, visitor authorization, equipment technician access, and custodian access. The access lists may take the form of typed pages, machine printed listings, business machine cards, or index cards. Information entered on the access list will include, where applicable, office room number, office telephone number, work hours, and area authorized to enter.

C. Access List to the Data Center

1. Use

The Access List to the Data Center may be used to clear employees for entry to FPP III after regular work hours (Section 2.B.2). This list is also used to clear employees for issuance of a Temporary Badge

(Section 4.H.1. and 2). An employee listed on the Visitor Authorization List may not sign another person into the Data Center if that employee is not at that time in possession of a properly issued Data Center Security Badge.

2. Additions

Only the Administrator, Systems Production Division, may authorize the addition of names to the Access List to the Data Center. When a Security Badge Application has been approved for an employee, the Administrator, Systems Production Division, will add the employee's name to the Access List to the Data Center.

3. Deletions

Bureau chiefs and division administrators are responsible for ensuring that names of their employees are promptly deleted when no longer authorized access to the Data Center. When an employee terminates employment with a division or for some other reason is no longer authorized for a Data Center Security Badge, the employee's division administrator or bureau chief must notify the Administrator, Systems Production Division, who will then remove the employee's name from the Access List.

D. Temporary Access List to the Data Center

1. The Temporary Access List to the Data Center also is used to clear employees for entry to the Data Center from 6:45 A.M. to 6:00 P.M. on regular workdays. This list may include names of persons for whom Data Center Security Badges have been requested and for persons working in the Data Center for a short period of time (Section 4.H.1). Persons whose names appear on this list will be issued a blue "T", Temporary badge (Section 4.H.2) without usual sign-in procedures (Section 2.A.2.d) for the times and days shown.

2. Additions

Only the Administrator, Systems Production Division, may authorize any addition to this list. Bureau chiefs and division administrators may inform the Administrator, Systems Production Division, of needed additions.

3. Deletions

Bureau chiefs and divisions administrators should advise the Administrator, Systems Production Division, of the names of any of their employees not needed on this list. The Administrator, Systems Production Division, will review this list approximately quarterly to assure deletion of names that may be beyond a stated expiration date. The Administrator, Systems Production Division, will notify the appropriate bureau chief or division administrator of the names of other persons whom it may be appropriate to omit.

E. Visitor Authorization List

1. Use

a. This list contains the names of persons who may authorize the issuance of an orange Visitor Badge (Section 5.A. and 5.B.3), a Temporary Badge (Section 4.H) or an Equipment Technician Badge (Section 5.A. and 5.B.1). The persons listed may clear persons for entry into the Data Center only for the categories of persons stated on the Visitor Authorization List. The Administrator, Systems Production Division, is responsible for maintaining the currency of the Visitor Authorization List in the manual of the Security Guard.

b. Visitors to the Data Center for purposes of touring the Computer Room will be authorized only by those management personnel shown on the Visitor Authorization List under the heading, "Management Group".

2. Additions and Deletions

Bureau chiefs and division administrators may request additions to the Visitor Autorization List. Such request should be made in writing to the Administrator, Systems Production Division. If the Administrator, Systems Production Division, deems the addition to be necessry, the Administrator, Systems Production Division, will take action to add the name(s) of the person(s) to the Visitor Authorization List. If the Administator, Systems Production Division, deems that the addition is not necessary, the request will be returned to the person forwarding the request with appropriate reasons stated. Should the person making the request deem the request is still fully justified and necessary, the matter may be referred to the Chief, Systems Processing Bureau, for resolution.

F. Equipment Technician Access List

1. Use

This list is used by the Security Guard to clear named individuals for issuance of a green Equipment Technician Badge (Section 5.B.1). An Equipment Technician Badge may be issued to persons named on the list without having an employee named on the Visitor Authorization List sign for them for the times and days shown.

2. Additions and Deletions

Bureau chiefs and division administrators may recommend to the Administrator, Systems Production Division, additions to the Equipment Technician List. The Administrator, Systems Production Division, is responsible for maintaining the currency of the Equipment Technician List in the manual of the Security Guard.

G. Custodian Access List

1. Use

This list is used by the Security Guard to authorize entry for custodians who work in FPP III after regular work hours. A Custodian Badge is issued to custodians working in the Data Center at any time (Section 5.B.2).

2. Additions and Deletions

The Assistant Commissioner for Business Management is responsible for approving custodian contractor employees at the beginning of each contract period and will provide a list of the employees to the Administrator, Systems Production Division. During the period of performance on the contract, requests for additions and deletions to the Custodian Access List may be forwarded by the custodian contractor to the Administrator, Systems Production Division, who may approve the changes. On approval of the changes, the Administrator, Systems Production Division, will provide the Security Guard an updated list of custodian contractor employees.

Section 4. Employee Access to the Data Center

A. General

1. Data Center Security Badge

   a. Designated employees of the Department are issued individually coded Data Center Security Badges for entry into the Data Center for specific work areas and times.

   b. Employees issued Data Center Security Badges include all employees whose normal work station is in the Data Center, selected staff of the Systems Development Bureau and the Systems Processing Bureau, and other persons authorized by the Chief, Systems Processing Bureau.

   c. For layout of the Data Center Security Badge see Attachment C.

2. Use of the Data Center Security Badge

   a. The Data Center Security Badge is a magnetically-coded plastic card which acts as a key to the electronic badge readers located at selected doors within the Data Center. It is coded for each employee's authorized time zone and status level (Attachment D), and, when inserted by the employee into an appropriate badge reader, is used to open doors into authorized work areas.

   b. The reader device located at the door of the computer room requires manual entry of a code along with the Data Center Security Badge. The code is given confidentially to each employee authorized entry to the computer room at the time that the Data Center Security Badge is issued. To protect the integrity of the security system this code must not be revealed to any other person.

3. Display of the Data Center Security Badge

   a. While in the Data Center, employees are required to wear the Data Center Security Badge on the front of their clothing above the waist, so that the photograph and color strip are visible.

   b. Employees are to be watchful of all persons inside the Data Center and challenge anyone not wearing a badge authorized for the work area where observed (refer to Section 6., Unauthorized Persons in the Data Center). Each Data Center Security Badge includes a color strip to indicate one of the following categories of access:

Color Strip	Work Areas
Yellow	Administrative
Green	Production Control Administrative
Blue	Computer Room Production Control Administrative
Red	Mail Room Administrative

4. Employee Responsibility for the Data Center Security Badge

   a. Each employee issued a Data Center Security Badge is responsible for safeguarding it, so as to prevent damage or loss.

   b. Lending of a Data Center Security Badge to any other person and borrowing of a Security Badge is not authorized.

   c. Precautions for protection and care of a Data Center Security Badge include:

      1) Not leaving it lying on desks or other places where it may be easily accessible to unauthorized persons.

      2) Not placing it in excessively warm places, especially in the sun and in closed cars, as excess heat will cause damage to it.

      3) Not allowing it to be abused by persons or animals that may cause damage to it.

B. Issuance of the Data Center Security Badge

1. Application Form and Approvals

   a. An Application for the Data Center Security Badge is required for:

      1) Initial issuance of a badge

      2) Change of a division in which employed

      3) Replacement of a lost badge

   b. A memorandum which requests a change in the time zone or status level coding, signed by the appropriate division administrator, or bureau chief, may be used in lieu of a completed application for a Data Center Security Badge that is issued to an employee.

c. For replacement of an unserviceable Data Center Security Badge, the employee issued the badge may turn it in to the Administrator, Systems Production Division, and request a replacement. A completed application or a memorandum signed by the appropriate division adminsitrator is not required when no other changes are needed. When a replacement Data Center Security Badge is issued appropriate notation will be made on the application.

d. Each employee to be issued a Data Center Security Badge must complete the first part of the application, TDHR Form 9124, (Attachment E), and forward it to the appropriate administrator, or to the highest level supervisor of the equivalent organization.

e. The employee's administrator (or highest level supervisor) will complete the approval portion for administrator, including assignment of proposed time zone and status level, and forward the application to the Administrator, Systems Production Division.

f. The Administrator, Systems Production Division, reviews each application for overall completeness including the requested access and time. If appropriate, the Administrator, Systems Production Division, may return an application to the division administrator of the employee with recommended revisions of access and time, along with the reasons for such recommendations.

g. If the Administrator, Systems Production Division, finds it approriate not to approve the application, the division administrator of the employee will be advised and reason for refusal stated. If the division administrator still feels a need for the employee to have a Data Center Security Badge, the application will be referred to the Chief, Systems Processing Bureau, with reasons for the refusal.

h. The Chief, Systems Processing Bureau, will take final action either to approve or to inform the division administrator of the employee stating the reasons for the refusal.

2. The Administrator, Systems Production Division

For each approved application, the following actions will be taken:

a. Add the employee's name to the Access List to the Data Center (Section 3.B.2).

b. Ensure that the employee's photograph is taken for the badge.

c. Issue an appropriately coded Data Center Security Badge and, if applicable, inform the employee of the additional code necessary for entry into the computer room.

d. Require the employee's signature stating that these Procedures were read and understood, and for receipt of the badge.

e. Enter in the remarks section of the application any other pertinent information.

f. Retain on file as confidential information the application of each employee who is issued a Data Center Secuirty Badge, along with any memoranda pertaining to the badge as authorized in Section 4.B.1.b) above. The application will be retained for not less than one year following the termination of the employee's authorization for the badge.

g. Maintain internal issuance records.

C. Failure to Bring the Data Center Security Badge to Work

An employee who fails to bring the Data Center Security Badge to work should advise the Police Officer who will contact the employee's supervisor. The supervisor, or other employee authorized to admit visitors, must then come to the police desk to identify and clear the employee for entry. The Police Officer may then issue a temporary badge to the employee in accordance with Section 4.H. below.

D. Lost Data Center Security Badge

1. Employee Report of a Lost Badge

An employee who loses or misplaces a Data Center Security Badge must report this fact to the supervisor and the Administrator, Systems Production Division, as soon as the loss is discovered, if during regular work hours. During non-regular work hours the employee should report the loss to the Police Officer.

2. Duties of Police Officer for a Lost Badge

The Police Officer will:

a. Note the report of a lost badge in the Daily Log (Attachment F);

b. Enter appropriate information concerning the lost badge on the list of Lost Data Center Security Badges kept at the police desk; and

c. Be alert to the possibility of an unauthorized person attempting to use the badge. This point is critical if the Administrator, Systems Production Division, has not yet had the opportunity to have the badge programmed out of the system.

3. Duties of Administrator, Systems Production Division, for a lost Data Center Security Badge

a. Reprogram the badge reader system to eliminate acceptance of that badge.

b. Ensure that a list of lost badges is kept at the police desk and is updated with appropriate information concerning lost badges.

c. Make a written notation in the remarks section of the application to indicate that the badge is lost.

E. Found Data Center Security Badge

1. Employee Action

An employee who finds a Data Center Security Badge should turn it in to the Police Officer as soon as practical.

2. Duties of Police Officer

a. Note receipt of the badge in the Daily Log (Attachment F);

b. Deliver the badge to the Administrator, Systems Production Division, as soon as possible;

c. Line through any reference to the found badge entered on the list of lost badges and initial and date it.

c. Line through any reference to the found badge entered on the list of lost badges and initial and date it.

3. Duties of Administrator, Systems Production Division, for a Found Data Center Security Badge

a. Ensure that any reference to the badge on the list of lost security badges has been lined through;

b. Determine if a new badge has been issued to the employee;

c. If a new badge has been issued, make a notation to indicate recovery of the badge in the remarks section of the application and ensure that the badge has been programmed out of the badge reader system;

d. If a new badge has not been issued but the employee is still authorized as a badge holder, return the badge to the employee after making a notation in the remarks section of the application to indicate recovery of the badge. Ensure that the badge reader system has been programmed to accept the badge as authorized.

e. If the badge is no longer authorized, ensure that the badge has been programmed out of the badge reader system. Make a notation in the remarks section of the appropriate application to indicate recovery of the badge.

F. Change of Duty Requiring Change in a Data Center Security Badge

An Application for a Data Center Security Badge (Form 9124) is required when an employee terminates employment with a division and accepts employment with another division, or when an employee's duties change so that different coding or a different color strip is required. The application is required to be submitted within ten regular work days of the effective date of transfer of the employee. If a different color strip is required, the badge must be turned in to the Administrator, Systems Production Division. Until receipt of the revised Data Center Security Badge, the employee may be admitted to the Data Center upon issuance of a Temporary Badge (Section 4.H).

G. Termination of a Data Center Security Badge Authorization

1. Action by the Employee

When an employee terminates empoyment or is requested to turn in a badge, the employee must do so.

2. Action by the Employee's Administrator (or Bureau Chief)

a. Immediately advise the Security Guard and the Administrator, Systems Production Division, to delete the employee's name from the Access List to the Data Center. (Section 3.B.3);

b. Forward the employee's badge to the Administrator, Systems Production Division, no later than the next regular work day following the employee's termination.

3. Action by the Administrator, Systems Production Division

a. Reprogram the badge reader system to eliminate acceptance of that Data Center Security Badge;

b. Ensure that the employee's name has been removed from the Access List to the Data Center; and

c. Make appropriate entries in badge issuance records.

H. Issuance and Use of a Temporary Badge

1. Circumstances for Use of a Temporary Badge

A Temporary "T" Badge (Attachment G) is bright blue in color and may be issued daily only to a person in one of the following categories:

a. An employee who fails to bring the Data Center Security Badge to work;

b. An employee seeking access at a time or to an area for which the Data Center Security Badge is not coded;

c. Employees awaiting issuance of a Data Center Security Badge who have been cleared for issuance of a Temporary Badge by a memo from the Administrator, Systems Production Division, to the Security Guard stating that an application for a Data Center Security Badge has been initiated; and

d. Persons working in the Data Center for a short period of time who have been cleared for issuance of a Temporary Badge by a memorandum from the Administrator, Systems Production Division, to the Security Guard adding the names of those persons to the Temporary Access List (Section 3.D).

2. Issuance of the Temporary Badge

Issuance of a Temporary Badge is a two-step process:

a. First, the Security Guard must ensure that the person is authorized for a Temporary Badge by locating the person's name on the Access List for the Data Center if the person is an employee who has failed to bring the badge to work or an employee seeking access at a time for which it is not coded. The names of persons working in the Data Center for a short period of time or awaiting issuance of badge will be identified on memos to the Security Guard (H.1. above).

b. A person authorized to admit visitors must go to the police desk and sign in the person seeking access to the Data Center. The Data Center employee authorizing issuance of the Temporary Badge should be from the area where the person will be working, and the name of the Data Center employee must be on the Visitor Authorization List maintained at the police desk. The Log of Visitors (Attachment A) is used to record information for a Temporary Badge.

c. If an employee, authorized to admit visitors to the Data Center, is not at that time in possession of a properly issued Data Center Security Badge, that employee may not sign any persons into the Data Center.

3. Display of the Temporary Badge

The Temporary Badge must be displayed on the front clothing above the waist at all times while the employee is in the Data Center. The badge must be turned in to the Police Officer at the end of the employee's work period in the Data Center each day.

I. Access at Times Other than Regular Work Hours

1. For access to normal work areas within the Data Center at a time for which the Data Center Security Badge is invalid, procedures for Issuance and Use of a Temporary Badge, Section 4.H. should be followed.

2. Employees Called to the Data Center

Employees may be called to the Data Center at night, on weekends or holidays, or at any time, to handle unexpected problems. If the employee called does not have a Data Center Security Badge coded for the time at hand, the Police Officer will notify the shift supervisor in the computer room when the employee arrives at the police desk. The Police Officer may admit the employee to the Data Center after the employee is properly signed in (Section 2). The employee must wear the Data Center Security Badge (or Temporary Badge) while in the Data Center. Upon leaving the Data Center, the employee must sign out with the Police Officer.

3. Access to the Documentation Center

The doors to the Documentation Center located in room 171 within the Data Center, are locked at all times other than during regular work hours. If an employee who is the holder of a current Data Center Security Badge requires entry to the Documentation Center when it is locked, that employee should request that the Police Officer unlock the door. The Police Officer will note the time and the employee's name in the Daily Log and unlock the door. The employee will wear the Data Center Security Badge (or Temporary Badge) while in the Data Center and promptly notify the Police Officer when access to the Documentation Center is no longer required. The Police Officer will relock the door, noting the time in the Daily Log.

4. Other conditions

Departmental employees who require access to the Data Center after regular work hours under any conditions other than above must be specifically cleared for entrance by the shift supervisor then on duty in the computer room or other employee whose name appears on the Visitor Authorization List (Section 3.D).

J. Access to Other Than Usual Work Areas

Access to other than usual work areas in the Data Center by an employee who is issued a Data Center Security Badge may be gained as follows:

1. The procedures stated in Section 4.H apply for issuance and use of a Temporary "T" Badge for an extended period of time.

2. For a brief period of time, an employee may request permission to enter an area from another employee who is issued, and at that time in possession of, and properly displaying, a Data Center Security Badge authorized for that area. If the employee to whom the request is made agrees to permit the employee making the request to enter, then that employee is responsible for all actions of the employee who enters, and must assure the exit of the employee.

3. The double doors on the north side of Production Control area may remain open during the regular day work periods 8:00 a.m. to 12 noon and 1:00 p.m. to 5:00 p.m. During the time that the Production Control area is open, any person, who is authorized access to the Data Center, may enter the Production Control area when on Departmental business. The provisions of Section 4.A.3.b, pertaining to challenge of unauthorized persons do not apply during these periods. These doors will be closed during the period 12 noon to 1:00 p.m. daily and at all times on weekends and holidays. When the doors are not open, access may be gained by use of an appropriately coded Data Center Security Badge.

Section 5. Visitor Access to the Data Center

A. General

1. Use of a Visitor Badge

   Anyone not possessing a valid Data Center Security Badge (or Temporary Badge) is required to obtain a Visitor Badge prior to entering the Data Center.

2. Categories of Visitor Badges

   Any of the three (3) different categories of visitor badges may be used. The type of badge issued is determined by the nature of the visitor's work in the Data Center.

3. Issuance of a Visitor Badge

   A visitor badge may be issued by the Security Guard whenever:

   a. The name of the individual seeking access is on one of the authorized access lists for visitors (Equipment Technician Access List or Custodian Access List)

   b. An employee authorized to admit visitors has gone to the security desk and signed in the visitor. Employees authorized to clear visitors are identified on the Visitor Authorization List kept at the guard desk.

4. Display of a Visitor Badge

   While in the Data Center, all visitors must wear the badge issued to them on the front clothing above the waist so that the badge is clearly visible.

5. Return of a Visitor Badge

   It is the responsibility of the person who cleared a visitor for entrance to ensure that the visitor badge is returned to the Security Guard as the visitor exits the Data Center.

B. Issuance and Use of a Visitor Badge

1. Equipment Technicians

   a. An Equipment Technician "E" Badge (Attachment G) is light green in color and is issued to persons servicing equipment in the Data Center. Equipment includes (but is not limited to) typewriters and other office equipment, telephones, fire detection and other monitoring systems, data entry equipment, and data processing and data communications equipment.

b. Equipment Technicians are cleared for entrance to the Data Center in either of two ways. The Security Guard may issue an Equipment Technician Badge to an individual named on the Equipment Technician List without further clearance. The Guard may require that the individual present personal identification to assure that the person is one named on the access list. Equipment Technicians may also be cleared for entry by an employee named on the Visitor Authorization List signing the appropriate space on the Visitor's Log.

c. A person wearing an Equipment Technician badge need not be escorted by an employee while in the Data Center.

2. Custodians

a. A Custodian "C" Badge (Attachment G) is gold in color and is issued to custodians working in the Data Center.

b. Custodians are cleared for entrance by reference to Custodian Access List kept at the security desk.

c. Custodians must be escorted by a Data Center employee while working in the production control area and in the computer room.

3. Visitors

a. A Visitor "V" Badge (Attachment G) is orange in color and is issued to persons visiting the Data Center who are not authorized for an Equipment Technician or a Custodian badge.

b. This type of visitor is cleared for entrance to the Data Center by an employee listed on the Visitor Authorization List going to the Security Guard's desk to sign in the visitor.

c. Any individual issued an orange Visitor Badge must be escorted by a person authorized to admit visitors or otherwise designated by the Administrator, Systems Production Division, while in the Data Center.

d. The employee who escorts the visitor is responsible for that visitor and is expected to be in visual contact with the visitor until the visitor has signed out and turned in his badge to the Security Guard.

C. Issuance of a Visitor Badge, Advanced Notice

1. Advanced Notice to the Security Guard

When a Data Center employee expects an official visitor, the Security Guard may be given advance notice of the visit as follows:

a. Supervisor authorizing the visitor;

b. Name of visitor;

c. Organization of visitor; and

d. Person or work area to be visited.

2. Admittance of Visitor to Data Center

Prior to admitting the visitor, the Security Guard will ensure that all appropriate information has been entered in the Daily Log and that the visitor is wearing the badge issued. The Security Guard will also inform the visitor that he must turn in his badge as he exits the Data Center.

D. Found or Unreturned Visitor Badge

1. Found Visitor Badge

a. If a Visitor Badge is found by an employee it should be turned in to the Security Guard immediately. On receipt of the Visitor Badge the Security Guard will notify the employee responsible for the visitor if the visitor is escorted. The employee must then go to the security desk with the visitor for re-issuance of the badge if the visitor is still present in the Data Center.

b. If the visitor is not escorted, the Security Guard will contact the supervisor of the work section where the visitor is working and request that supervisor to direct the visitor to the security desk to have the Visitor Badge re-issued.

2. Unreturned Visitor Badge

If a visitor departs the Data Center and does not return the Visitor Badge, the Security Guard will note that fact on the Log of Visitors and also make an entry in the Daily Log. The Administrator, Systems Production Division, will assist the Security Guard in recovering an unreturned Visitor Badge.

E. Authorization to Admit Visitors by the Computer Room Shift Supervisor

The computer room shift supervisor is authorized to admit visitors to any area of the Data Center when no employee whose name is on the Visitor Authorization List is then working in the Data Center. The shift supervisor is responsible for a visitor so admitted during the time that the visitor remains in the Data Center.

Section 6. Unauthorized Persons in Data Center

A. Employee Action

An employee should advise a supervisor, or manager, or the Security Guard, if a person in the Data Center appears not to be authorized access, as follows:

1. Not displaying a Data Center Security Badge color coded for the area (Section 4.A.3), unless accompanied by, and in the immediate vicinity of, a person displaying a Data Center Security Badge color coded for that area (Section 4.J).

2. Not displaying a temporary type badge.

3. Not in the vicinity of an employee observing the person, if that person is displaying a Visitor Badge (Section 5.B.3).

4. Not in the vicinity of an employee observing the person, if that person is displaying a Custodian Badge in the production control area or the computer room (Section 5.B.2).

B. Supervisory Action

If the supervisor determines that the person has not been authorized entrance to the area, the supervisor will take appropriate corrective action as follows:

1. Employee Not Authorized in the Area

   If the person is an employee not authorized to be in the area where observed, the supervisor will report the incident to the employee's supervisor who will take additional action as necessary.

2. Person Not Authorized in the Data Center

   If a person is observed who has not been authorized entrance to the Data Center, a supervisor or manager employee will accompany the individual to the security desk. The Security Guard will notify the Administrator, Systems Production Division, of the unauthorized entry and prepare a report of the incident (Attachment H, Capitol Security Police Activity Summary). The Administrator, Systems Production Division, will report the incident to the Chief, Systems Processing Bureau (Section 1.B.5).

3. Removal of an Unauthorized Person

   In extreme cases, the Security Guard may be requested to remove an unauthorized person from the Data Center.

Section 7. Use of Monitored Doors

A. General

1. Description

   There are nine (9) doors in the Data Center/FPP III which are equipped with monitoring devices. When any of the monitored doors are opened without authorization, these devices sound an alarm at monitor panels both at the security desk at the east and in the computer room on the south wall.

2. Monitored Doors in the Data Center

   Monitored doors in the Data Center (#1 - #7, Section 7.B) remain activated unless deactivated as allowed by these Procedures (Section 7.C).

3. Monitored Doors in FPP III

   Monitored doors in FPP III are activated by the Security Guard as follows:

   a. South door, FPP III, #9, is activated each regular work day at 6:00 P.M. when the door is locked, and is deactivated each regular work day at 6:45 A.M. when the door is unlocked.

   b. East door, FPP III, #8, is activated only when the Security Guard is away from the security desk during the following times:

      1) After 6:00 P.M. and before 6:45 A.M. on regular work days

      2) Anytime on weekends and holidays.

B. Location of Monitored Doors

The following doors are monitored (Attachment I):

1. Rear exit door, east-west corridor, Data Center
2. Rear door to the mail room (#196), Data Center
3. Rear door to forms handling room (#197), Data Center
4. Rear door to forms storage room (#199-E), Data Center
5. Rear door to computer room (#199), Data Center
6. Door to motor generator room outside rear computer room door, Data Center
7. Door to electrical switch room inside the mailroom (#196), Data Center
8. East door, FPP III
9. South door, FPP III

C. Action for Door Usage

1. Use of a Monitored Door

   a. Department employees who regularly work in the Data Center and are issued a Data Center Security Badge may request that a door be deactivated.

   b. An employee who has work which requires use of any of the monitored doors may contact the Security Guard, either in person or by telephone to request that the specific door be deactivated. The door should not be opened until the Security Guard has authorized the employee to do so.

   c. In emergency situations, such as a fire alarm or other conditions in which danger is considered imminent, persons may exit a monitored door without prior clearance from the Security Guard. When such an exit is made, the persons so exiting should carry out the following actions:

      1) Guard the entrance so as to prevent unauthorized persons from entering the Data Center.

      2) Report the reasons for exiting, as soon as practicable, to the Security Guard and the supervisor of the area.

2. Request for Authorization to Open Door

   a. The Security Guard should be given the employee's name, telephone number, reason the door is to be opened, and estimated length of time the door is to be in use. The Security Guard will note this information in the Daily Log.

   b. If an employee requires use of a door for an extended period of time, the employee requesting that a door be deactivated must confirm continued use of the door to the Security Guard approximately each thirty (30) minutes.

   c. If the door is opened for deliveries or other purposes involving use of the door by non-employees of the Data Center, those persons must first report to the Security Guard for issuance of a visitor badge.

3. Verification by the Security Guard

   The Security Guard must be assured that a request is legitimate before authorizing use of a door and may verify a request by one of the following actions:

   a. Call the employee on the telephone for location and identification

   b. Require the employee to come to the security desk

   c. Go to the door area to make an on-location determinatio.

4. Authorization to Open Door

When satisfied that the request is legitimate, the Security Guard will advise the employee that the door may be opened.

5. Responsibility of the Requesting Employee

It is the responsibility of an employee who requests that a door be deactivated from the door monitor system to assure that:

a. Any door in the door monitor system is not left unattended.

b. Another employee is designated to attend the door, if the employee who requested that the door be deactivated cannot attend that door at all times when it is open.

c. Any person who enters the Data Center through a deactivated door has been issued a temporary type badge by the Security Guard.

d. No person in possession of a Security Badge is allowed to enter a door deactivated from the door monitor system who has not previously exited from that door while engaged with work in process at that time.

e. Any temporary type badge is turned in to the Security Guard on completion of work for which it is issued.

f. Doors are firmly shut and latched when entry through the doors are no longer required.

g. The Security Guard is notified when use of the door is no longer required.

6. Reactivation of Door Monitor

The Security Guard will note in the Daily Log the time when notified to reactivate the monitor on a door that has been temporarily deactivated. If the Security Guard is not notified to reactivate the door monitor within the estimated use time, the Security Guard will contact the requesting employee to determine if the door is still in use. If not, the Security Guard will reactivate the door monitor, note in the Daily Log the time and the fact that the Security Guard was not informed when use of the door was no longer required.

D. Action at Alarm

1. Alarm Conditions

Alarm conditions are indicated at each monitoring panel by the horn sounding and the red "ALARM" button(s) lighting for the appropriate door(s).

2. Cause of Alarm

Alarm conditions may be caused by:

a. Unauthorized entry though a monitored door;

b. A malfunction within the system; or

c. Certain attempts to disable the system, such as cutting a wire.

3. Action of the Security Guard

When alarm conditions are indicated, the Security Guard should go immediately to the appropriate door and determine the cause. If the door activating the alarm is the rear door to the computer room or to the forms storage room the shift supervisor in the computer room should also go to that door immediately. If necessary, the Security Guard on duty will call for assistance from the Capitol Security Police Operations desk or the Austin Police Department.

4. Information to Data Center Personnel

After the problem has been resolved, the Security Guard should inform appropriate Data Center personnel of the conditions causing the alarm and the corrective action taken. Depending upon the situation, persons to be informed may include the supervisor of the work area adjacent to the door; the shift supervisor in the computer room; the Administrator, Systems Production Division. As soon as practical, the Security Guard will make an entry in the Daily Log describing the alarm situation and detailing action taken in resolving the problem.

E. System Malfunction

1. Temporary Deactivation of a Door From the System

If an alarm is activated, but a physical check of that door indicates that the alarm was caused by a malfunction within the system, the Security Guard will use the monitor panel at the security desk to temporarily remove the appropriate door from the monitoring system. The Security Guard should also notify the shift supervisor in the computer room to deactivate the appropriate door on the monitor in the computer room. A monitor panel should never be unplugged as a means of deactivating all doors simultaneously, as this action may drain the backup battery power.

2. Report of Malfunction

Any malfunction which occurs should be reported to the Security Guard. During normal work hours the Security Guard will notify the Administrator, Systems Production Division, who will contact the Door Monitor maintenance contractor to request remedial maintenance (refer to Attachment J). If critical malfunctions occur during other than regular work hours, the Security Guard will contact the maintenance contractor (refer to Operating Instructions for Door Monitoring System in the Security Guard manual).

Section 8. Fire Prevention, Detection, Evacuation and Other Emergencies

A. General

1. Fire Detection and Alarm System

   a. FPP III

      The fire alarm system consists of:

      1) Manual fire alarm pull stations of:

         a) Near the elevator on the first floor of the two-story building, and

         b) In the hallway near the north (double door) entrance to the production control area in the Data Center.

      2) Alarm bells with flashing lights located:

         a) Near the elevator on the first and second floors of the two-story south portion of the building, and

         b) In the hallway near the north (double door) entrance to the production control room of the Data Center.

   b. Data Center

      The fire detection and alarm system consists of ionization detectors, photo electric smoke detectors, manual fire alarm pull stations, and alarm bells with flashing lights at specific locations (Attachment I). It includes two surveillance panels; one surveillance panel is located at the police desk and one surveillance panel is located on the south wall of the computer room.

2. Fire Drills

   Fire drills, either announced or unannounced, will be conducted by the Chief, Systems Processing Bureau, not less than semi-annually, during which all persons should exit the building by the most direct fire evacuation route (Attachment I), closing doors to offices if last to leave. The elevator must not be used during an emergency evacuation of FPP III.

3. Fire Prevention and Safety Measures

   a. Each employee should know the most direct routes and alternate routes out of FPP III away from any area of danger.

   b. Each employee should know the location of the nearest fire extinguisher to the normal work area and be able to activate it to extinguish a fire.

c. Supervisors will ensure that flammable trash accumulated in a work area is placed in one of the covered metal trash receptables or other appropriate containers for that area. Computer room supervisors should ensure that liquids, particularly flammable liquids, not be placed on any piece of equipment.

d. All employees should be alert to any dangerous, or potentially dangerous situation, and, if noted, call the supervisor's attention to it immediately.

e. No Smoking should be enforced by supervisors/managers of work units.

1) Smoking is not permitted in:

a) Mail room, 196

b) Electrical/Telephone room, off room 196

c) Equipment Room, 102

d) Elevator

2) Smoking is permitted only in designated parts in the:

a) Mail vault in room 196

b) Forms handling room (break area), 197

c) Computer room (break area), 199

d) Tape library (break area), 199-C

e) Forms storage room (break area), 199-E

f. Burned or partially-burned smoking materials should be disposed of only in containers marked for this purpsoe. Such materials should not be disposed of in waste paper baskets or other containers in which flammable materials are placed.

4. Fire Extinguishers

The Chief, Systems Processing Bureau, is responsible for assuring that regular employees of the building receive training annually in the proper use of fire extinguishers.

B. Fire Alarm Actions

In the event that the alarm sounds and/or the warning lights flash in work areas or at either of the surveillance panels for any area, the

following actions will be taken in a rapid and orderly manner by the Security Guard and also by the supervisor in any area of alarm:

1. Action Sequences

   a. Determine the location of the fire from a surveillance panel or by observing flames or smoke.

   b. Go immediately to the place of the alarm (Attachment I), or the fire.

   c. If a fire is present, attempt to extinguish it with the nearest fire extinguisher, if appropriate.

   d. If danger exists:

      1) Pull the manual fire alarm. The Security Guard is responsible for alerting persons to danger and pulling the manual fire alarm for that portion of the building where an alarm has not been set off. The nearest manual fire alarm pull stations to the Security Guard at the east door are located as follows:

         a) For the FPP III, two-story south portion: near the elevator on the first floor.

         b) For the Data Center: inside and to the right of the east door of room 194, Data Entry.

      2) Direct all persons to depart from the building by the most direct fire evacuation route away from the area of danger (Attachment I). The elevator must not be used in an emergency.

      3) Telephone the Austin Fire Department at 476-4333. The Security Guard will advise the Capitol Security Police Force by telephone and request emergency assistance if necessary.

      4) Supervisors should make certain that:

         a) All persons evacuate the building, and that

         b) Employees in the next closest work unit are alerted.

      5) Supervisors are responsible for disconnecting electrical equipment and cutting off electric light switches in each work area if time permits. For cutoff of the data processing and terminal equipment, see Attachment K.

      6) Close each door after determining that the area is no longer occupied by any person.

7) Assist all employees in leaving the building by the closest evacuation route to the outside away from the area of danger (Attachment I). Special assistance should be given to any person with any physical disability such as a hearing or sight impairment or lack of full leg mobility. The Security Guard will take action to unlock and open both Security Badge reader controlled doors at the main entrance to the Data Center.

8) Direct, or designate an employee to direct, arriving fire fighters to the fire.

e. If successful in extinguishing the fire, inform the following persons:

1) Employees in the area

2) Administrator, Systems Production Division, if during a regular day shift

3) Supervisor in the computer room at times other than regular day shift, if the Security Guard is first to respond

4) Security Guard, if a supervisor is first to respond

5) Capitol Security Force desk officer, by the Security Guard, as soon as practical (#475-2208).

2. Action Responsibilities

a. In event of an alarm in more than one area, supervisors should respond to an alarm in their area of responsibility first in accordance with instructions in Section 8.B.1 above.

b. The Security Guard will provide maximum assistance to persons in the area of greatest danger.

c. The Security Guard should make an entry in the Daily Log (Attachment F) and file an Activity Summary (Attachment H).

d. Employees are expected to take actions as follows:

1) Move rapidly out of the building and not attempt to take personal articles

2) Assist other employees, and

3) After reaching the outside, move away from the building and stay out of the way of emergency vehicles and persons.

C. Malfunction of the Fire Detection and Alarm System

1. Malfunction of the System

a. During normal work hours the Security Guard will notify the Administrator, Systems Production Division, who will contact the maintenance contractor (Attachment J) to request remedial maintenance.

b. During other than normal work hours, for critical malfunction, the Security Guard will contact the maintenance contractor (Attachment J) (refer to Operating Instructions for Fire Detection and Alarm System in Security Guard manual).

2. Action During Malfunction

The Security Guard will silence audio alarms and will notify the appropriate supervisor in the area which has the malfunctioning devices. The supervisor should be especially watchful of the area involved until malfunctioning components are again fully operational.

D. Other Emergencies

1. Personal Illness or Accident

a. For emergency medical assistance, the following units and persons should be contacted and the condition of the person needing help should be described (see Attachment R):

1) Austin Emergency Medical Service (EMS), #474-1911; (The EMS is in immediate contact with and will dispatch when needed the Austin Fire Department Resuscitator Unit, #476-4333)

2) Unit or organization supervisor

3) Security Guard

a) Regular daytime work hours, #443-7711, ext. 100; For emergencies: 443-7711, ext. 300

b) Other than regular daytime work hours, #443-2737; For emergencies: 443-2747

c) The emergency numbers for the Security Guard should be used only for that purpose and should be answered immediately by the Security Guard.

b. For immediate assistance in the treatment of accidents, any person may contact the Security Guard and the persons on the Listing for Emergency Treatment (Attachment L).

c. For minor accidents, First Aid assistance may be given by the Security Guard, and by supervisors and qualified persons in areas in which First Aid Kits are available, as follows:

1) Security Guard's desk

2) Data Entry area, room 194-B

3) Production Control area, room 195-A

4) Computer console desk, room 199

5) Computer shift leader, room 199-B

6) The open area opposite room 148

7) Administrative area, room 202

d. Reporting of accidents

1) Accidents should be reported by persons who know the circumstances, to the following persons:

a) The Security Guard

b) The appropriate supervisor in the division, or bureau, where the accident occurs.

2) The facts provided should include description of injuries, name of witnesses, time and place, medical assistance and other known information.

3) Record of information and reports for each accident will be completed by persons as follows:

a) Security Guard: Activity Summary (Attachment H)

b) A Department employee appointed for the purpose: reports as required by the Department Administrative Management Handbook, Section 9420: Accident Reporting.

2. Severe Weather Danger

In event of severe weather danger, as announced by supervisors, employees should move away from outside windows and other glass partitions, using the interior corridors and inside rooms for protection.

3. Explosive or Other Threat of Destruction

a. Employees who answer telephones should pay close attention to, and make notes about the following elements concerning any telephone call which includes a threat:

1) Exact information of what the caller says, including

a) Location of the device

b) Time the device is to be set off

c) Type and description of the device

d) Reasons for the threat.

2) Clues as to the caller's identity: age, sex, voice characteristics, accents, background noises, and any other information that may be of interest or importance.

b. An employee who receives a threat of potential danger should report the incident to a supervisor immediately.

c. The supervisor should advise the Security Guard of the threat and accompany the employee to the division administrator, bureau chief, or other appropriate manager. The employee will then advise the manager of the threat.

d. The manager may decide that FPP III should be evacuated. If so, the manager should inform the Security Guard of the situation and ensure that the nearest fire alarm pull station is activated to set off the fire alarms.

e. All persons will evacuate the building, using the fire evacuation routes (Attachment). The elevator must not be used during an emergency evacuation of FPP III.

f. The Security Guard will:

1) Request assistance from the Capitol Security Police bomb disposal unit, if appropriate.

2) Ensure that the fire alarms have been activated in both the south and north portions of the building; and

3) Provide other appropriate assistance to aid in the evacuation.

g. As soon as practical, the employee who received the threat should assist the Security Guard in recording all data about the threat. Examples of Capitol Security Police forms used for this purpose are shown at Attachment M, Threatening Phone Call Form, and Attachment N, Description of Caller's Voice.

4. Other Emergency

For any other emergency, such as flood, earthquake, explosions or fire outside of the building, employees are expected to react pursuant to instructions of appropriate supervisors and managers.

E. Emergency Units, Admittance

1. The Security Guard is expected to render appropriate assistance to emergency units which are called to the Data Center.

2. The Security Guard is authorized to admit persons of an emergency unit into the Data Center while that unit is in performance of an emergency mission. Persons that may be so admitted are limited to those performing duties connected with fire fighting, medical service, law enforcement or other emergency that may require rescue or protection of life, limb or property. Such persons or units may be admitted only after verification of an actual emergency.

Section 9. Miscellaneous Procedures

A. Restrictions on Animals and Vehicles

1. Access to FPP III is not authorized for animals, except for "Seeing Eye" dogs. Only vehicles, such as carts and dollies, used in Department business are authorized in FPP III.

2. Animals and vehicles are not authorized to be tied or chained in any way that interfere with easy entrance and exit of the building.

B. Restrictions of FPP III Area

1. The Security Guard, at 6:30 P.M. each regular work day, will attach a barrier chain with the restrictive sign stating, "Do Not Enter" across the alley entrances at the northeast corner and the southwest corner of the building, and will remove the chains at 6:30 A.M. each regular work day.

2. These chains will remain attached during weekends and holidays except when removed by the Security Guard for Department business.

C. Restrictions on Custodians

1. Custodians may not bring into FPP III unknown or inappropriate substances, objects or packages and may be searched by the Security Guard to assure compliance with this restriction.

2. Custodians may not remove from FPP III any Department property.

3. Custodians may not open a door controlled by a door monitor (Section 7) unless the Security Guard is present at the door when it is opened.

D. Parking Lot Lights

1. The parking lot lights are normally activated by a photo-electric cell external to FPP III.

2. In the event of failure, and the lights do not come on at dark, the Security Guard will turn on the manual switch which is on the north wall of the inner partition of the electrical/telephone room located off the Mail Room, #196; this switch is marked "PARKING LOT LIGHTS OVERRIDE SWITCH".

E. Automobile Identification

1. Employees who regularly drive vehicles to work and park them in the FPP III parking lot and adjacent areas are expected to provide information on an Automobile Identification card, DHR Form 9127 (Attachment O), for each car driven. The information includes make, color, model, year, license, owner, and telephone number. These cards may be obtained from each bureau and division administrative section in FPP III and from the Security Guard.

2. The completed card will be retained in a file maintained by the Police Officer. It will permit the Police Officer, or an appropriate manager, to notify employees for any of the following reasons: lights are left on, vehicle is parked in an unauthroized place, when a vehicle is parked in or near a place where work is in progress on the building, lot or street, or other useful reasons.

F. Parking of Vehicles, FPP III

1. Persons who park vehicles in the FPP III area are expected to show courtesy and observe the rights of others. No person may restrict the flow of traffic by the manner in which a vehicle is parked, or otherwise park in an unauthorized area.

2. Persons may park vehicles in the FPP III parking lot in any unrestricted parking space. Head-in parking only is permitted adjacent to the east side of the Data Center and along the fences to the west of FPP III.

3. Various parking places are restricted and designated as no parking, service vehicles, visitors, motorcycles, bicycles, handicapped, reserved, and State vehicles. Parking restrictions do not apply after 5:00 P.M. and before 7:00 A.M. on regular work days, or anytime on weekends or holidays, to the following spaces only: visitors, services vehicles, and reserved. Parking is permitted at all times only for the designated purposes in the following spaces: handicapped, bicycles, and motorcycles. Parking is not permitted at any time in the driveways or along curbs painted yellow or in any spaces marked "No Parking".

4. When space is available,

   a. Persons authorized to use the retricted parking spaces for service vehicles, handicapped, reserved and State vehicles are required to park in the spaces designated.

   b. Persons who ride motorcycles are expected to park in the space so designated, or other authorized place in which a car cannot park.

   c. Persons who ride bicycles are expected to park in the space so provided, at or near the rack for bicycles.

5. Unauthorized Parking

   For unauthorized parking the following procedure will be followed:

   a. The Police Officer will:

      1) Place on the vehicle a written notice stating the violation (Attachment P).

2) Record the violation on the back of the Automobile Identification card (Section 9.E).

3) Inform the Administrator, Systems Production Division, of any second and subsequent parking violation.

b. The Administrator, Systems Production Division, will refer repeated violations by an employee to the appropriate division administrator or bureau chief for corrective action.

G. Action of Security Guard When Away From East Door

When the Security Guard is away from the security desk at the east door:

1. These actions apply during the following hours:

   a. On regular work days, prior to 6:45 A.M. or after 6:00 P.M., and

   b. On weekends and holidays at anytime.

2. The Security Guard will follow this sequence of actions:

   a. Inform the computer room shift supervisor of the absence from the security desk, the reason for the absence, and the expected time of return.

   b. Lock the east door and place an appropriate sign on it stating that the officer will return in the near future.

   c. Activate the door monitor on the door monitor panel for the east door.

3. On return to the security desk the Security Guard will follow this sequence of actions:

   a. Inform the computer room shift supervisor

   b. Unlock the east door and remove the sign

   c. Deactivate the door monitor on the door monitor panel for the east door.

4. The Security Guard will make entries as appropriate in the Capitol Security Police Daily Log (Attachment F).

H. Data Center Check by Security Guard

The Security Guard will make a security check:

1. Of the Data Center, by a physical walk-through within one hour of departure of the custodial crew, with special attention to Monitored Doors 1, 2, 3, and 7 (Section 7.B.).

2. Of the alley to the west side of FPP III, by visual observation each hour,

   a. Tuesday - Saturday, 2:00 A.M. - 6:00 A.M.

   b. Saturday, Sunday and holidays during hours of darkness

3. As a part of these security checks the Security Guard should comply with these Procedures, Section 9.G.

I. Emergency Contacts and Notifications

During other than regular work hours, it may be necessary to seek information from, or provide information to, specified employees of the Data Center and FPP III. Should such a situation occur, the Security Guard and the Shift Supervisor of the computer room will first confer so as to assure that each is aware of the matter at hand, then either may contact the persons shown on the specified list of employees for Emergency Contacts and Notifications (Attachment Q). Situations in which it may be necessary to contact these persons include the following:

1. A problem not covered by these procedures and not otherwise reasonably resolvable.

2. A condition which may cause danger to employees, or a situation that may lead to destruction of equipment.

3. Any action which has caused damage to equipment or injury to an employee.

ATTACHMENTS

A. Log of Visitors, TDHR Form 9125

B. Building Register, TDHR Form 9126

C. Data Center Security Badge (Layout)

D. Badge Access Levels

E. Application for Data Center Security Badge, TDHR Form 9124

F. Capitol Security Police Daily Log (Capitol Security Police form)

G. Data Center Temporary Type Badges (Layout)

H. Capitol Security Police Activity Summary (Capitol Security Police form)

I. Emergency Evacuation Routes, Location of Emergency Equipment

J. Security Systems Maintenance Contractor Firms

K. Power Cutoff of the Data Processing and Terminal Equipment

L. Employee Listing for Emergency Treatment of Accident or Illness

M. Threatening Phone Call Form (Capitol Security Police form)

N. Description of Caller's Voice (Capitol Security Police form)

O. Automobile Identification card, TDHR Form 9127

P. Unauthorized Parking Notice

Q. Emergency Contacts and Notifications

R. Emergency Telephone Numbers

S. Evacuation Plan, FPP III

State of Texas
Department of Public Welfare

Form 9125
June 1977

LOG OF VISITORS, DATA CENTER
(Log runs midnight to midnight)

_____, 19___.
Day of the week Date

Please print all information

Badge Number	Names		Visitor's Organization	To Visit/Work			Turn in	
	Authorized by	Visitor		Person/Purpose	Area	Time	Time	S. G.

Texas Department of Human Resources

Form 9126
October 1977

BUILDING REGISTER, DATA CENTER

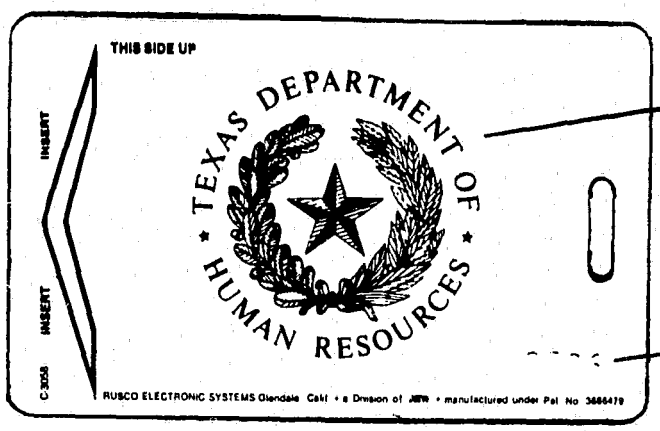
Please print all information

TWO STORY BLDG.

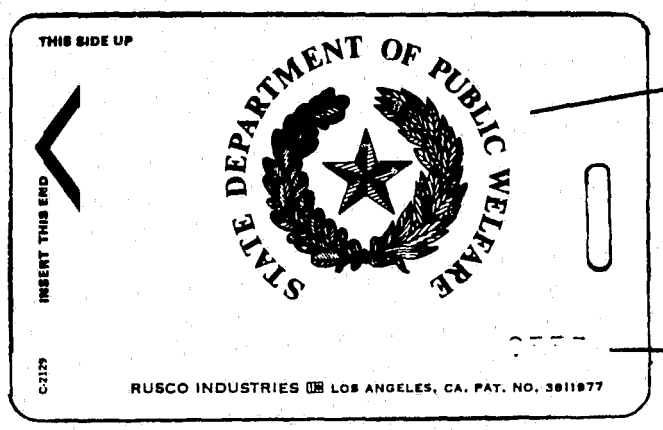
DATE	PRINT NAME	ORGANIZATION	ROOM NUMBER	TIME IN	TIME OUT	REMARKS

DATA CENTER SECURITY BADGE

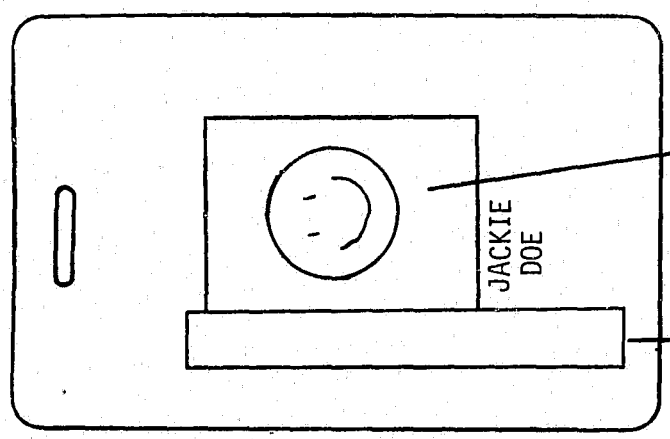
FRONT



FRONT (Alternate badge)



BACK



BADGE ACCESS LEVELS

The access level assigned to each badge consists of two components: (1) Time Zone and (2) Status Level.

TABLE 1
Time Zone

The time zone indicates the time period each day for which the badge is valid.

Time Zone	Time Valid
1	6:45 a.m. - 6:00 p.m.
2	3:30 p.m. - 2:00 a.m.
3	10:30 p.m. - 9:00 a.m.
4	24 hours

TABLE 2
Status Levels

The status level designates badge-controlled doors which are accessible to the badge holder.

Status Levels	Doors					
	(1) Front	(2) Prod. Control (Single)	(3) Prod. Control (Double)	(4) Mail Vault	(5) Forms Vault	(6) Comp. Room
1	x					
2	x	x	x			
3	x	x	x			x
4	x	x	x		x	x
5	x			x		

Texas Department
of Human Resources

Form 9124
May 1978

APPLICATION FOR DATA CENTER SECURITY BADGE

REQUESTED FOR:

Name (Last Name First)	Job Title	
Work Area	Normal Work Hours	Telephone No.

Signature–Applicant _____ Date _____

APPROVED BY:

Time Zone	Status Level

Signature–Administrator _____ Date _____ Division Name _____

Signature–Chief of Systems Processing Bureau _____ Date _____

ISSUED TO:

Color Strip	Code

I have read and understand the Physical Security Procedures, Data Center, FPP III,

and I acknowledge receipt of security badge number _____.

Signature–Applicant _____ Date _____

Issued by:

Signature–Security Representative _____ Date _____

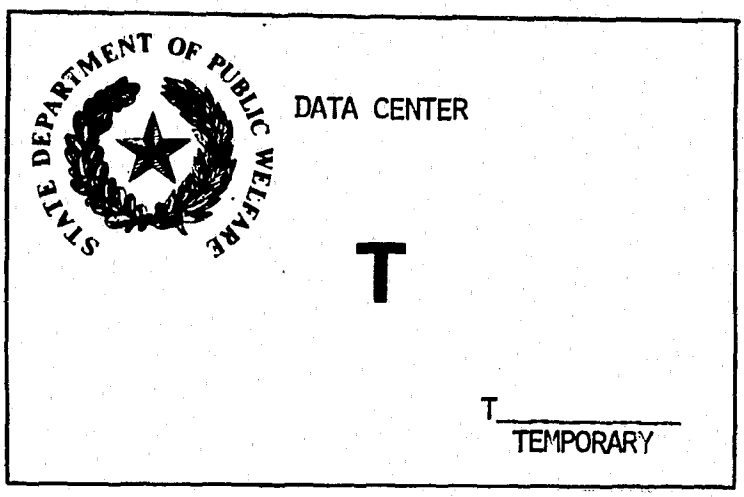
REMARKS:

CAPITAL SECURITY POLICE DAILY LOG

DATE: **SHIFT:** **PAGE:**

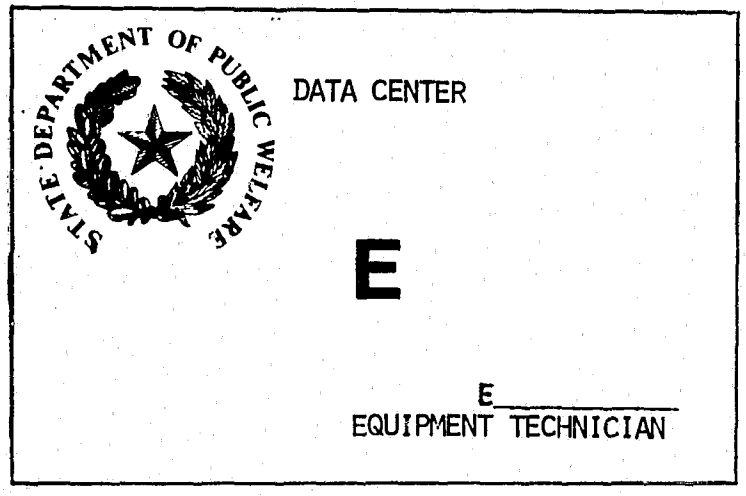
ITEM #	TIME:	INCIDENT:	REMARKS OR DETAILS:	OFFICER:

Data Center
Temporary
Type
Badges



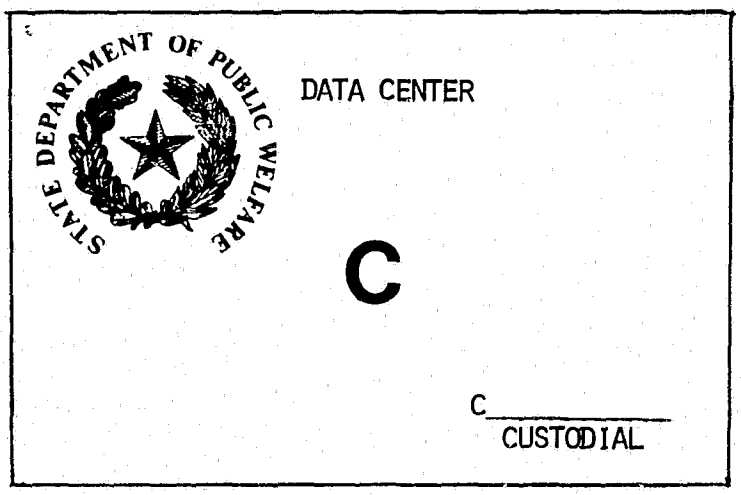
Color,
Bright Blue

Badge
Number



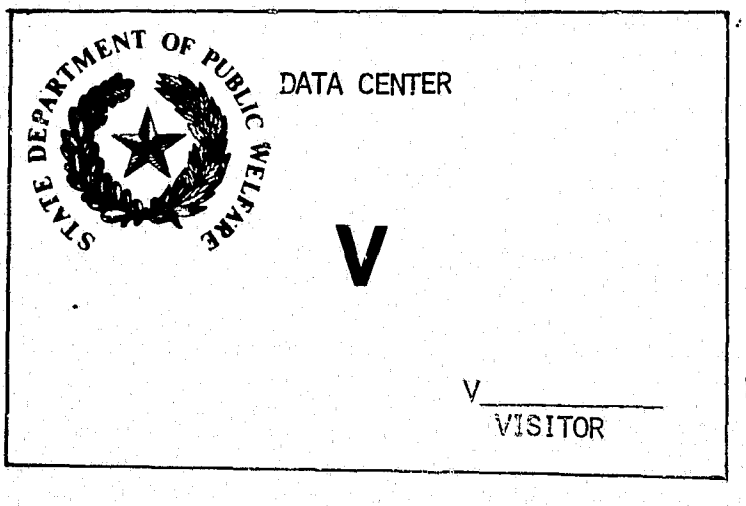
Color,
Light Green

Badge
Number



Color,
Gold

Badge
Number



Color,
Orange

Badge
Number

ACTIVITY SUMMARY

BC—164

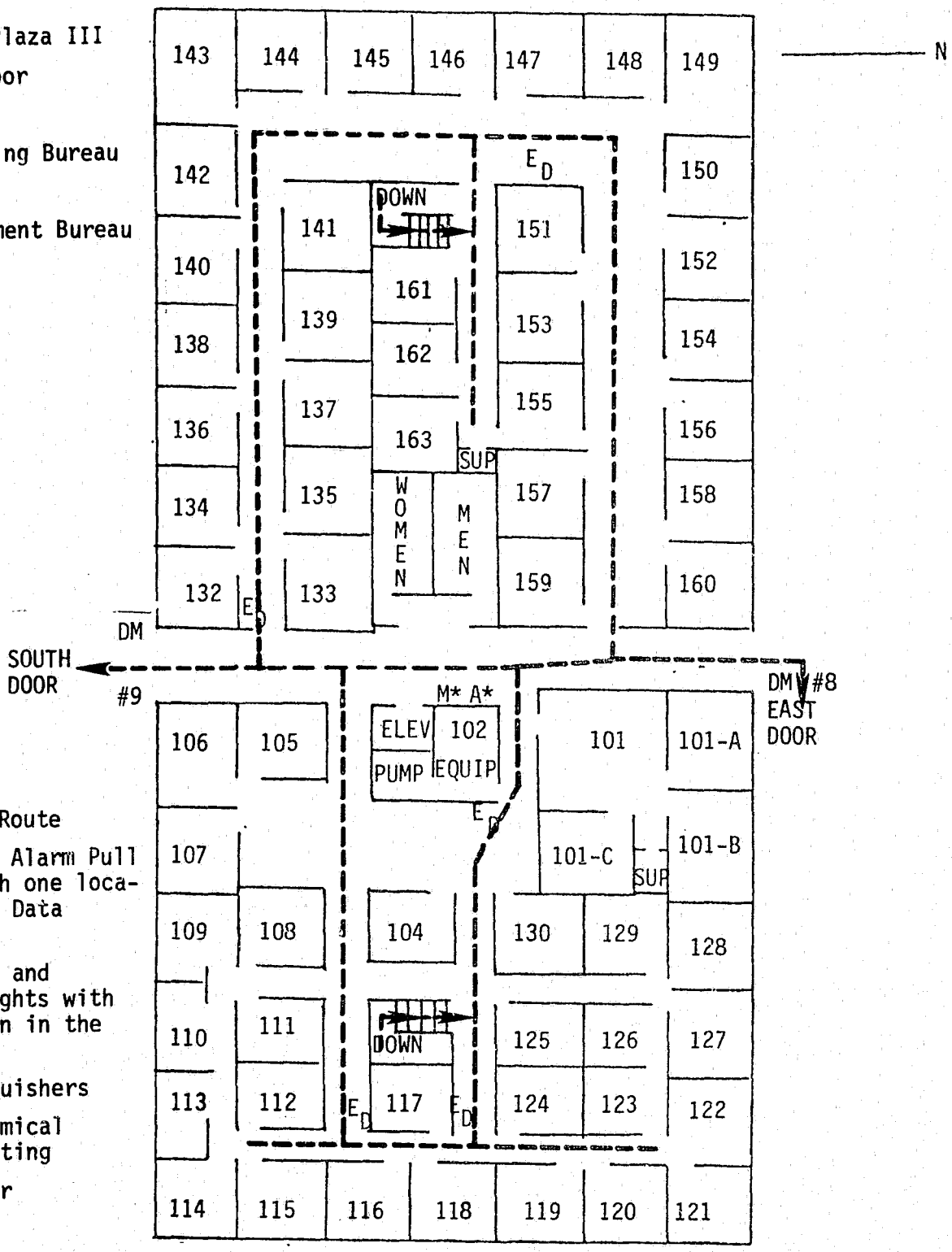
CR SA NBPD 1/1/69 10

1. FILE NO.	2. COMPLAINANT ADDRESS	3. PHONE BUS. RES.
4. ACTIVITY TYPE		5. REPORTED BY PERSON ( ) SIGHT ( ) PHONE ( ) RADIO ( ) LETTER ( )
6. LOCATION		
7. REPORTED BY		
12. DESCRIBE ACTIVITY REPORTED - OR DISCOVERED NARRATIVE: GIVE NAMES & ADDRESSES OF PERSONS INTERVIEWED		8. DATE & TIME COMMITTED
		9. RECEIVED BY
		10. DATE & TIME RECEIVED
		11. DATE & TIME OFFICER ARR.

REPORTING OFFICER	REPORTING OFFICER	TIME & DATE OFFICER'S REPORT RECEIVED IN CENTRAL REC.
NAME OF SUP. OFFICER APPROVING REPORT	TIME & DATE APPROVED	NAME C.R. CLERK RECEIVING OFFICERS REPT.

EMERGENCY EVACUATION ROUTES
Location of Emergency Equipment

Fountain Park Plaza III
First Floor
TDHR
Systems Processing Bureau
and
Systems Development Bureau

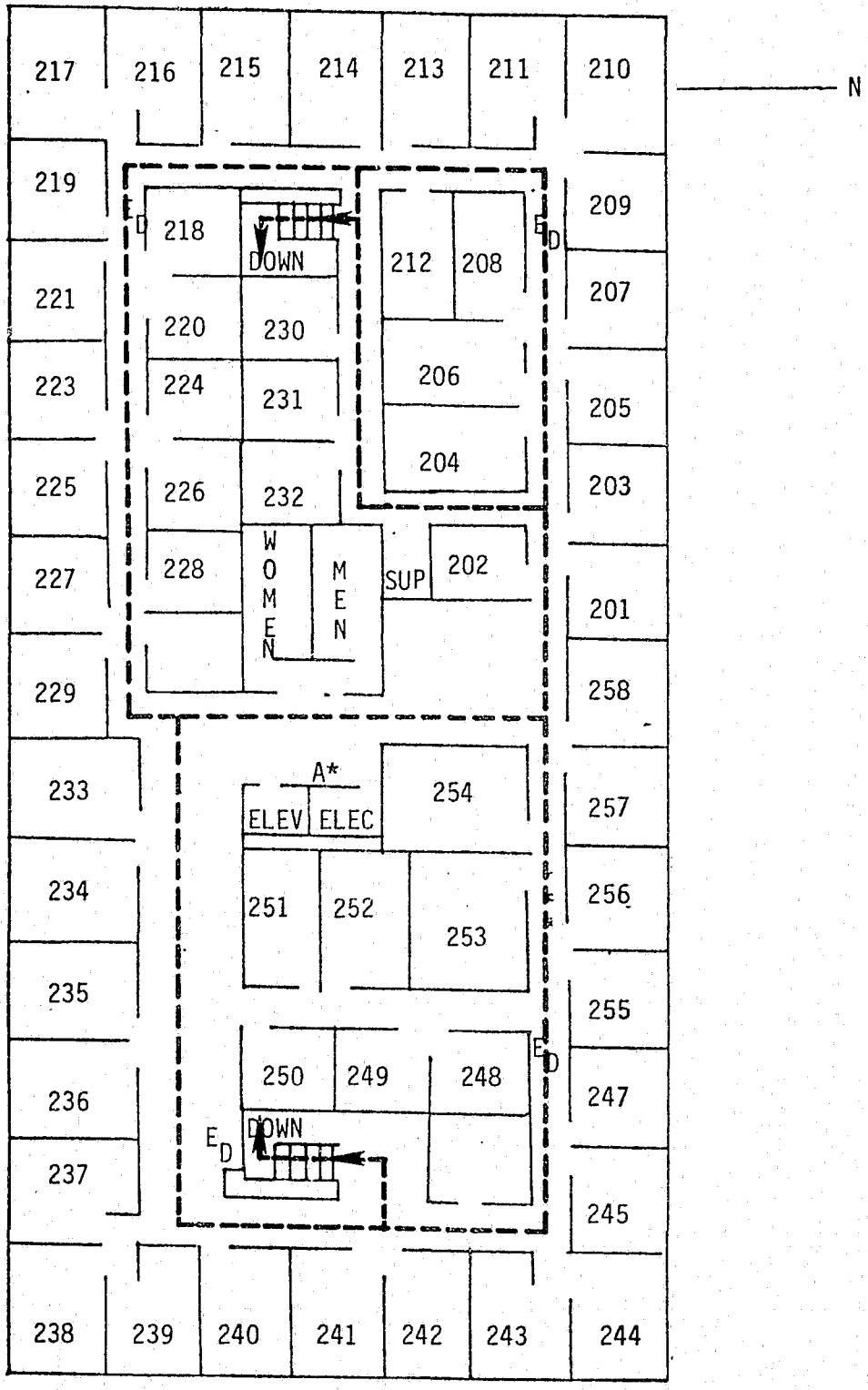


LEGEND

- Evacuation Route
- M* Manual Fire Alarm Pull Station with one location in the Data Center
- A* Alarm Bells and Flashing Lights with one location in the Data Center
- E Fire Extinguishers
  - D - Dry chemical ABC rating
- DM Door Monitor

EMERGENCY EVACUATION ROUTES
Location of Emergency Equipment

Fountain Park Plaza III
Second Floor
TDHR
Systems Developement Bureau



LEGEND

——— Evacuation Route

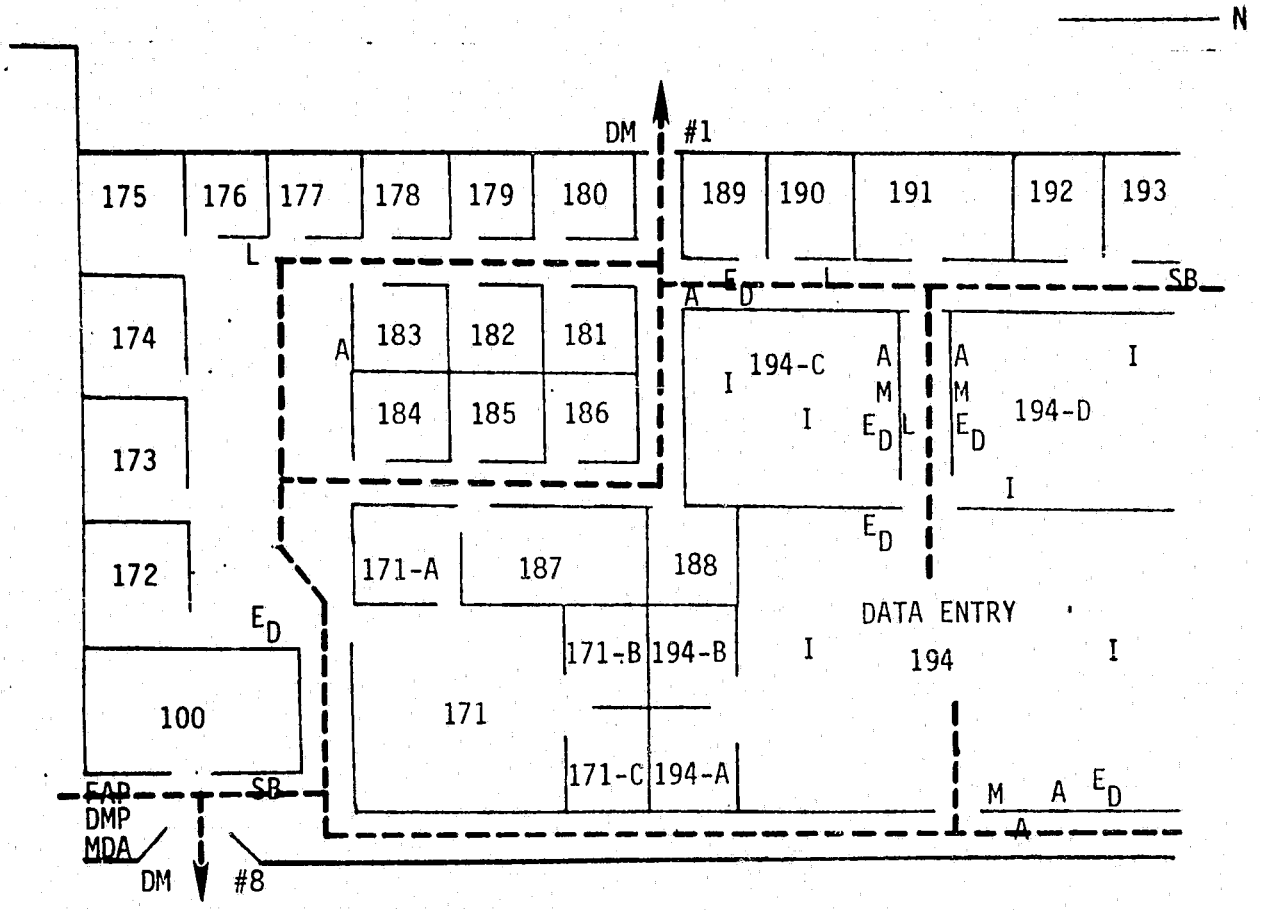
A* Alarm Bells and Flashing Lights, with one location in the Data Center

E Fire Extinguishers

D - Dry chemical ABC rating

Elevator may not be used in an emergency.

EMERGENCY EVACUATION ROUTES
Location of Emergency Equipment
Data Center
Fountain Park Plaza III, TDHR

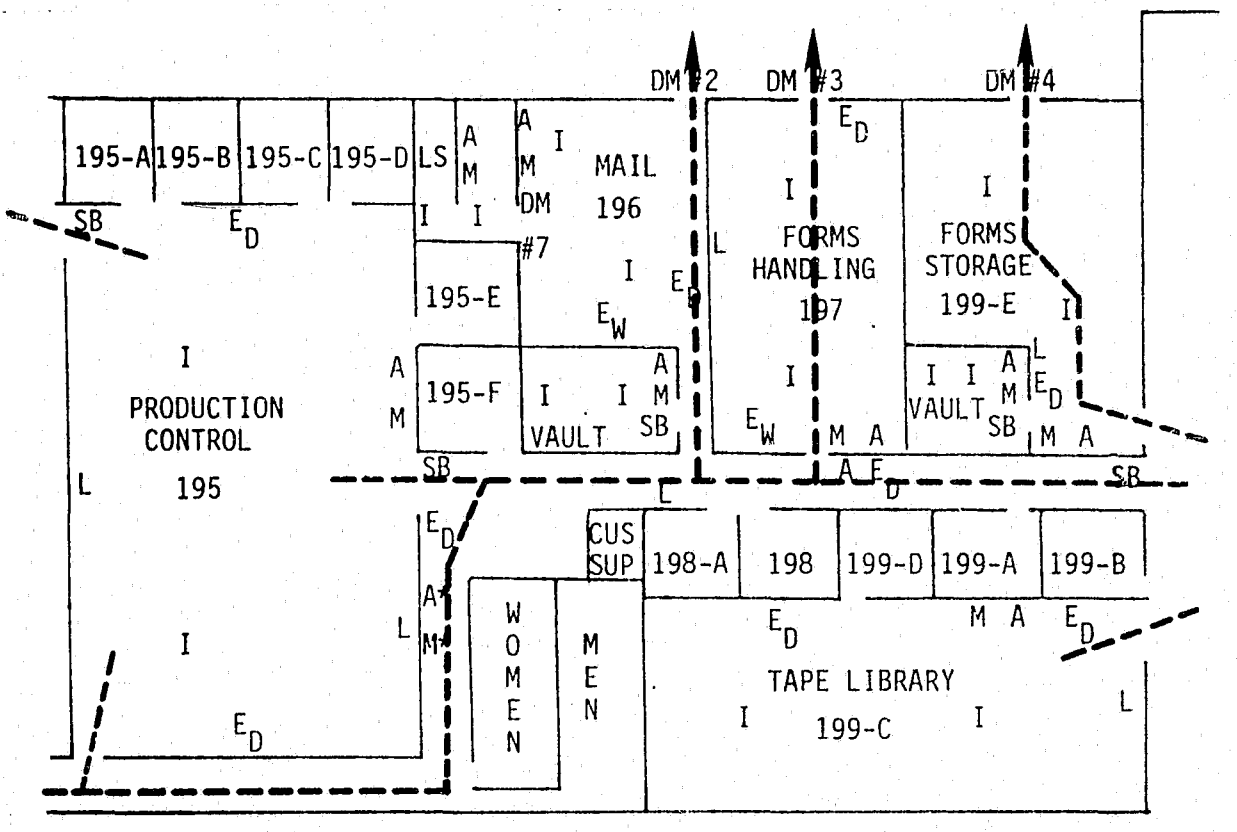


LEGEND

- Evacuation Route
- L Emergency lights
- FAP Fire Alarm Panel
- M Manual Fire Alarm Pull Station, Data Center
- A Alarm Bells and Flashing Lights, Data Center
- I Ionization Detectors
- DMP Door Monitor Panel
- DM Door Monitor
- MDA Moisture Detector Alarm
- SB Security Badge Controlled Door
- E Fire Extinguisher
  - D - Dry chemical ABC rating

EMERGENCY EVACUATION ROUTES
Location of Emergency Equipment
Data Center
Fountain Park Plaza III, TDHR

N



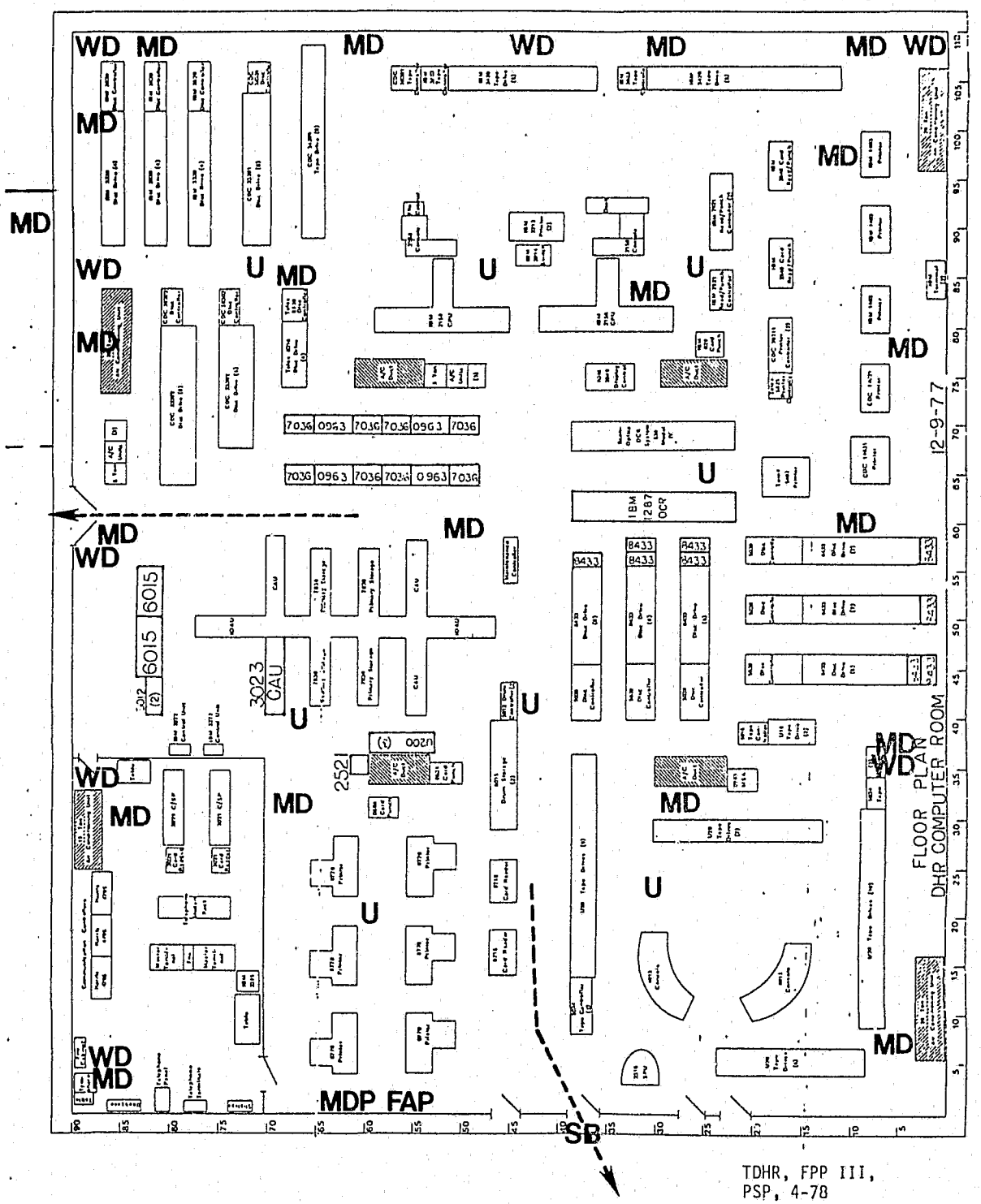
LEGEND

- Evacuation Route
- L Emergency Lights
- M Manual Fire Alarm Pull Station, Data Center
- A Alarm Bells and Flashing Lights, Data Center
- M* Manual Fire Alarm Pull Station, FPP III; one location in the Data Center
- A* Alarm Bells and Flashing Lights, Data Center
- I Ionization Smoke Detectors, Ceiling
- DM Door Monitor
- SB Security Badge Controlled Door
- LS Parking Lot Lights Override Switch
- E Fire Extinguishers
  - D - Dry chemical, ABC rating
  - W - Water, A rating

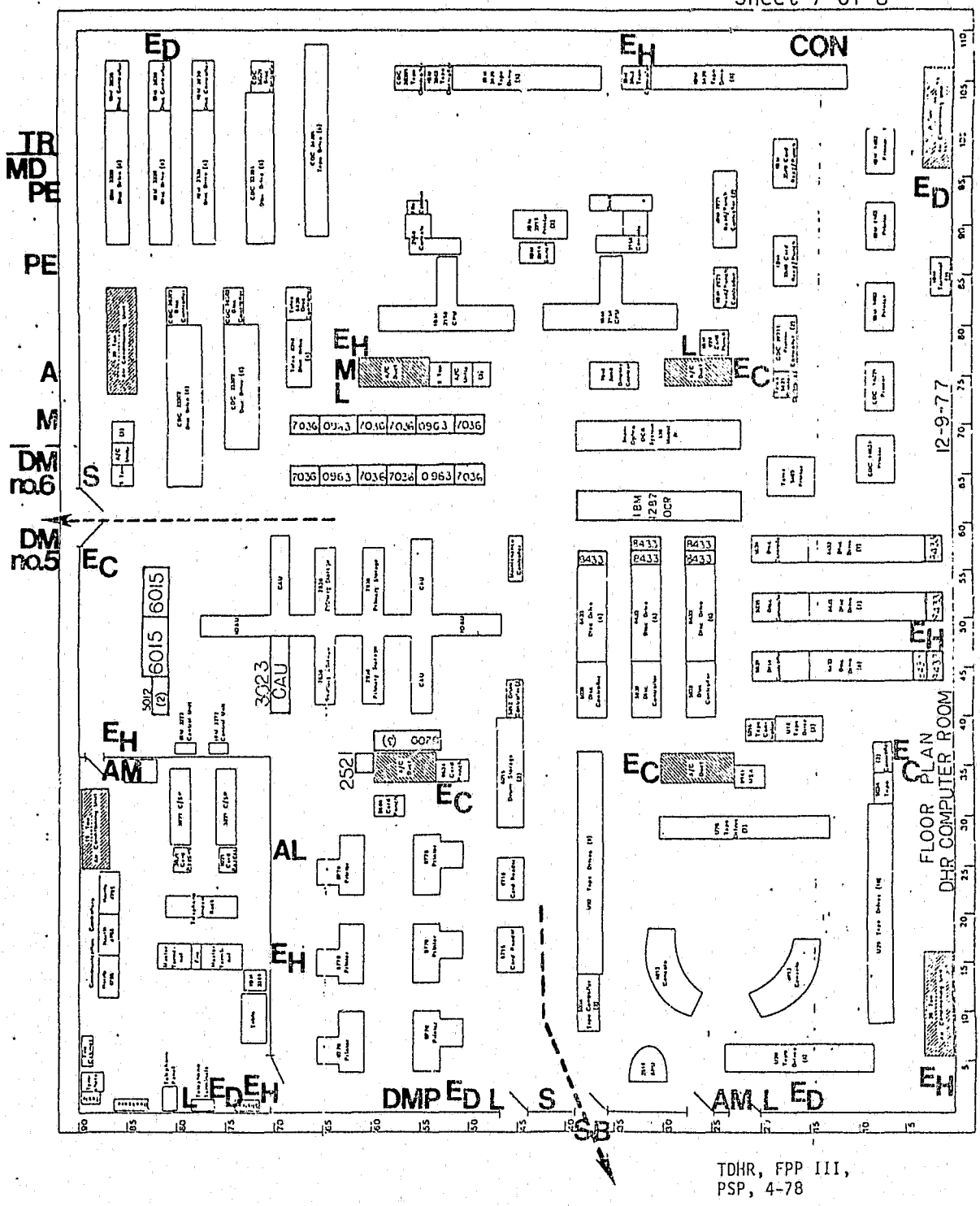
LEGEND

(See accompanying diagrams)

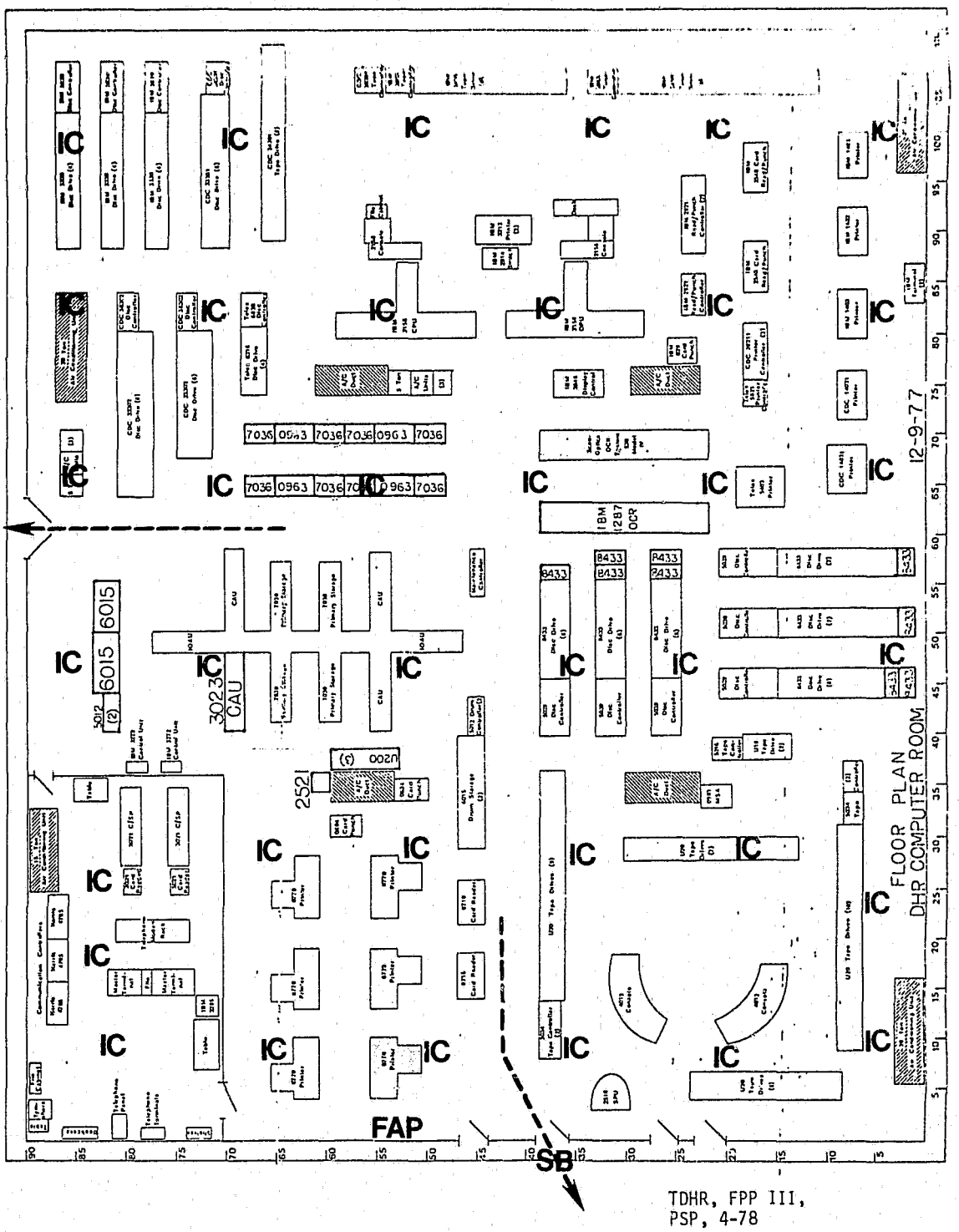
----	Evacuation Route
L	Emergency Lights
M	Manual Fire Alarm Pull Station, Data Center
A	Alarm Bells and Flashing Lights, Data Center
S	Switch for emergency power cut-off
DM	Door Monitor
DMP	Door Monitor Panel
AL	Alarm for water sump pump, Transformer room
CON	Security Badge Console
SB	Security Badge Controlled Door
FAP	Fire Alarm Panel for IC, PE, U and WD
IC	Ionization Smoke Detectors, Ceiling
PE	Photo-Electric Smoke Detectors, Transformer Room Ceiling
U	Ionization Detectors, Under-floor
WD	Water Detector, Under-floor
MDP	Moisture Detector Panel with Alarm
MD	Moisture Detector, Under-floor
TR	Transformer room
E	Fire Extinguisher
	D - Dry chemical, ABC rating
	C - CO_2, Carbon dioxide, BC rating
	H - Halon, ABC rating



TDHR, FPP III,
PSP, 4-78



TDHR, FPP III,
PSP, 4-78



TDHR, FPP III,
PSP, 4-78

Attachment J

SECURITY SYSTEMS MAINTENANCE CONTRACTOR FIRMS
Service Telephone Numbers

System Description	Maintenance Service (Reg. Work Hrs.)	Emergency Service (Non-reg. wk. hrs.)
Security Badge reader (6 doors)	Annandale Service Co. 451-7531 4200 Medical Parkway,Rm.201 Austin, TX 78763 (Mr. McQuown)	Mr. Al McQuown 451-7531
Fire Detection and Alarm Notifier; Data Center Door Monitor (9 doors) Water Detector (computer rm., under floor	Tele Systems 345-1727 P.O. Box 4355 Austin, TX 78765 (Mr. Samaniego)	Mr. Bob Samaniego 345-1727
Fire Detection and Alarm, Simplex; FPP III/Data Center Air Conditioning, Carrier Units on Data Center Roof Air Conditioning, Lennox Units in Computer Room Electrical, IBM	Property Management and Development Co. 476-7028 106 East 9th Street Austin, TX 78701 (Mr. Martine)	Mr. Tom Martine 476-7028
Air Conditioning, Data-Aire Units in Computer Room Air Conditioning, Condensate Sump Pump, Transformer rm. Moisture Detector, Supreme-Aire	Fox Service Company 442-6782 1500 Stassney Lane Austin, TX 78745	Fox Serv. Co. 442-6782
Electrical, Sperry Univac	AA Electric Company 442-2667 2321 S. Lamar Blvd. Austin, TX 78704 (Mr. Tanner)	Mr. Glen Tanner 442-2667
Air Conditioning, Trane Unit in Computer Room	V. R. Wattinger, Inc 282-0616 114 Slaughter Lane Austin, TX 78745 (Mr. Wattinger)	Mr. Ron Wattinger 453-7039
Air Conditioning Compressor Monitoring System	McCown Electric 442-8392 2708 Sherwood Lane Austin, TX 78704	N/A

NOTE: Refer to Section 3.F. and 5.E. for authorization to enter Data Center.

POWER CUTOFF OF THE DATA PROCESSING AND TERMINAL EQUIPMENT

The first priority during emergency conditions for evacuation of FPP III is the safety and protection of persons. Therefore, all persons should depart FPP III by walking swiftly and in a direct route but away from any area of danger.

When practicable, evacuation from the computer room may include cutting off power to the data processing equipment by activating an emergency cutoff switch. There are two of these switches. Each may be identified as a red button recessed in a gray box and labeled, "EMERGENCY CUT-OFF SWITCH". The switches are located:

1) On the south wall to the right of the single door which leads into the hallway, and

2) On the west wall to the right of the double doors leading out of FPP III into the alley.

Activation of either of these emergency cutoff switches will immediately stop electrical power to the data processing equipment in the computer room. Therefore an "EMERGENCY CUT-OFF SWITCH" should be used only during real emergency conditions, such as:

1) Danger to life or limb necessitating an emergency evacuation.

2) Actual smoke or flames in the computer room.

3) Immediate danger of explosion or other hazard.

For situations in which time is less critical than during an actual emergency, the procedures attached should be followed as listed below:

System	Attachment
1) IBM 370/158	K-2
2) Univac 1100/43	K-3
3) Terminal equipment	K-4

Power-down and cut off procedure for:

IBM Systems 370/158

If time permits, take the following action before activating the "EMERGENCY CUTOFF SWITCH".

First: Depress the STOP button on each computer console.

Second: Depress the POWER-OFF button on the 370/158.

Notes: (1) Depressing the power-off button will permit a cycle down of all system components and permit resumption of processing when the emergency is cleared.

(2) DO NOT pull the EMERGENCY POWER-OFF knob that is on the computer unless the computer is the source of the fire.

Power-down and cut off procedure for:

Univac Systems 1100/43

The following is the general guide for powering down the Univac system.

Notes: 1) This list will serve as a guide to each component in turn.

2) Each component has a mark on the door, behind which is listed the power down procedure for that particular cabinet.

Unit	Item/Quantity	Unit	Item/Quantity
Uniservo 20's	32 each	CAU-Ø	Cabinet #1
MAS 14	Cabinet #90	CAU-1	Cabinet #2
MAS 13	Cabinet #100	IOAU-0	Cabinet #11
MAS 16	Cabinet #110	CAU-2	Cabinet #4
MAS 15	Cabinet #120	CAU-3	Cabinet #3
8433 Disc Drives	63 each-Turn Off each drive at Operators panel by releasing start button.	IOAU-1	Cabinet #12
		Main Store 0/1	Cabinet #21
		Main Store 2/3	Cabinet #23
		Main Store 4/5	Cabinet #25
		Main Store 6/7	Cabinet #27
MAS 6	Cabinet #330	Extended Store Ø	Cabinet #31
MAS 5	Cabinet #340	Extended Store 1	Cabinet #32
MAS 8	Cabinet #350	MAI Ø	Cabinet #30
MAS 7	Cabinet #360	Extended Store 2	Cabinet #41
MAS 10	Cabinet #370	Extended Store 3	Cabinet #42
MAS 9	Cabinet #380	MAI 2	Cabinet #40
MAS 12	Cabinet #310	Extended Store 4	Cabinet #51
MAS 11	Cabinet #320	Extended Store 5	Cabinet #52
1782 Drum	Cabinet #401	MAI 4	Cabinet #50
1782 Drum	Cabinet #411	Extended Store 6	Cabinet #61
MAS 1	Cabinet #400	Extended Store 7	Cabinet #62
MAS 2	Cabinet #410	MAI-6	Cabinet #60
1782 Drum	Cabinet #421	SPU-MAS Ø	Cabinet #71
1782 Drum	Cabinet #431	Console Ø	Cabinet #81
MAS 3	Cabinet #430	Console 1	Cabinet #82
MAS 4	Cabinet #420	GSC	Located on the end of MAS 4
Uniservo 16	Cabinet #240		
Uniservo 16	Cabinet #241	Maint. Controller	Located in front of CAU-1
Uniservo 16	Control Cabinet #130		
MAS 17	Cabinet #131	Uniscope 200	4 each including tape library push power on/off button.
0770 Printers	6 each		
0716 Card Readers	2 each		
0604 Card Punch	2 each	Cop Printer in tape library	
Printer Transfer Switch	Cabinet #550		
C/SP-20	Cabinet #511		
C/SP-19	Cabinet #501		

Power-down and cut off procedure for:

Terminal Equipment Outside of the Computer Room

1. If time permits, turn off the circuit breaker at the power supply panel which services that equipment.

2. The second best alternative is to power down the equipment and then unplug it from the wall outlet:

   a. Bell telephone equipment: unplug from wall (no on/off switch).

   b. Gandalf line driver: power off by flipping toggle switch on front of unit.

   c. IBM

      1) Terminals: power off by pushing in the power switch located in the lower left corner of front face.

      2) Printer/Control Units: power off by flipping toggle switch located in recess on left front of equipment.

   d. Univac

      1) Terminal Multiplexor: power off by flipping toggle switch on front.

      2) Controller/terminals: power off by flipping toggle switch located on the front under the screen.

      3) COP printer: power off by flipping toggle switch located on right front of the equipment.

      4) Printer 0786: power off by pushing on/off button on right front top of the printer.

Attachment L

FPP III EMPLOYEES WITH TRAINING IN EMERGENCY MEDICAL TREATMENT PROCEDURES

NAME	OFFICE TP# 443-7711 (WORK HRS)	OFFICE ROOM #	TRAINING PROVIDED BY	TYPE OF TRAINING	DATE OF TRAINING
FIRST SHIFT					
Bob Craig (Complete trauma kit and resuscitator in car)	X 261 8 AM-5 PM	219	UT AHA	Registered EMT Instructor, CPR	5-77 2-78
James L Brown	X 159 8 AM-5 PM	159	ARC AHA	FA, CPR CPR	6-77, 7-77 7-77
David Fuson	X 114 7:30 AM - 4:30 PM	114	AHA ARC	CPR FA	5-78 6-78
Liz Berru	X 177 8 AM-5 PM	177	ARC	FA	7-77
Lea Erb	X 345 8 AM-4 PM	199 Cmptr Rm	ARC	FA	7-77
Gary Holmes	X 242 7:30 AM - 4:30 PM	242	ARC	FA	6-77
Dion Melton	X 160 8 AM-5 PM	160	ARC	FA	6-77
Mike Pierce	X 340 8 AM-5 PM	199C Tape Lib'y	ARC	FA	7-77
Jerry Ross	X 219 8 AM-5 PM	219	AHA	CPR	9-78
Olivia Rountree	X 323 8 AM-5 PM	194D Data Entry	ARC	FA	7-77
SECOND SHIFT					
Gary Gillespie	X 346 4 PM-12 Mn	199 Comptr Rm	EMS	ECA	4-78

LEGEND:
FA - First Aid
CPR - Cardiopulminary Resuscitation
ARC - American Red Cross
AHA - American Heart Association
EMT - Emergency Medical Technician
ECA - Emergency Care Attendant
EMS - Emergency Medical Service

TDHR, FPP III,
PSP, 3-79

THREATENING PHONE CALL FORM

Time call received _____ **Time caller hung up** _____

Exact words of person placing call: _____

_____

_____

_____

_____

_____

Questions to Ask:

1. **When is bomb going to explode?** _____

   _____

2. **Where is the bomb right now?** _____

   _____

3. **What kind of a bomb is it?** _____

   _____

4. **What does it look like?** _____

   _____

5. **Why did you place the bomb?** _____

   _____

Person (receiving) (monitoring) call _____

Dept. _____ **Telephone No** _____

Home Address _____

Home Telephone No. _____

Date _____

DESCRIPTION OF CALLER'S VOICE

Male _____ **Female** _____

Young _____ **Middle Age** _____ **Old** _____

Tone of Voice _____

Accent _____

Background Noise _____

Is voice familiar? _____

If so, who did it sound like? _____

Remarks: _____

State of Texas
Department of Public Welfare

Form 9127
November 1976

AUTOMOBILE IDENTIFICATION

MAKE	COLOR	
MODEL	YEAR	LICENSE
OWNER		TELEPHONE NO.

Attachment P

UNAUTHORIZED PARKING NOTICE

TEXAS DHR
FPP III

Date _____ Time _____ License # _____

Violation - Improper parking in space of:

- ☐ Service vehicle
- ☐ Visitor or handicapped
- ☐ Motorcycle or bicycle
- ☐ No parking
- ☐ Other _____

NOTE:
1. A record will be kept of this notice.
2. Repeated instances of unauthorized parking will be reported to your supervisor.

_____
Officer, Capitol Security Police

TDHR, FPP III
PSP, 4-78

Attachment Q

Telephone list (home) of employees for
EMERGENCY CONTACTS AND NOTIFICATIONS
(Persons should be contacted in the order stated)

Systems Production Division

Ms. Gloria Winn	441-2512
Mr. Jimmie Chance	258-2595
Mr. John Robertson	345-9614
Mr. Dick Reich	441-5239

Systems Processing Bureau

Mr. James Logan Brown	345-4007
Mr. Ray Lester	928-3577
Mr. Dean Jessen	282-2397

Personnel Section

Mr. Louie Stearns	441-5219

Systems Management

Mr. Bill Stobie	443-6771

Systems Development Bureau

Mr. Owen Ware	345-1723
Ms. Mary Awbrey	836-5145
Mr. Tommy Huntress	255-2350

Analysis and Programming

Ms. Marguerite Abel	285-3114

Technical Development

Mr. Pat Roach	444-8263

Medical Systems

Mr. Art McDonald	836-5131

Financial Systems

Mr. Hank Atkinson	441-6830

Attachment R

EMERGENCY TELEPHONE NUMBERS

Austin Fire Department	FIRE DEPT	9-476-4333
Austin Emergency Medical Service	EMS	9-474-1911
Austin Police Department	POLICE	9-476-8311
Capitol Security Police (State Capitol)		9-475-2208
Security Guard (east door):		
Regular work daytime hours		443-7711
Regular line		Ex. 100
EMERGENCY line		Ex. 300
Other than regular work daytime hours		
Regular line		443-2737
EMERGENCY line		443-2747
Computer Room		
Regular work daytime hours:		443-7711
IBM		Ex. 345
S-U		Ex. 346
Other than regular work daytime hours		
IBM		443-2867
S-U		443-2868

PLAN FOR EVACUATION OF FPP III

Introduction

A. In the event of evacuation of FPP III for emergency reasons, it is important that assistance is provided:

1) to any employee needing assistance,
2) for protection of equipment, property, and data, and
3) so that all persons may depart FPP III safely by a direct route and in a rapid manner.

Therefore, specific employees occupying named organizational positions, as well as certain other categories of employees, are assigned duties at, during and following an emergency evaluation of FPP III.

B. This Plan for Evacuation consists of three parts as follows:

Section I, FPP III evacuation during regular day work hours.
Section II, FPP III evacation during other than regular day work hours.
Section III, Duties of the Police Officer, Capitol Security Police (CSP).

Section I. This section applies to a building evacuation during regular weekday work hours, 8 a.m. to 5 p.m. (See Diagram, Schematic, attached). General managers of the organizations listed in this section, the bureau chiefs and division administrators, will designate by name the appropriate employees for the functions indicated. Recapitulation of the designation of stations is attached for reference.

A. FPP III and surrounding area, Station 1 (Generally, to the east and south of FPP III)

1. Responsible Managers

Title	Organization	Names
Chief	Systems Processing Bur. (SPB)	_____
Assistant Chief	SPB	_____
Administrative Assistant	SPB	_____
Administrator	Technical Support Div. (TSD)	_____
Administrator	Systems Management Div. (SMD)	_____

2. Responsibilities of Managers

   a. Control all FPP III area and employees
   b. Ensure clearance of employees from FPP III
   c. Locate in view of south or east door; keep door entrance guard employees informed of location
   d. Report status of whole FPP III area and OIS employees to Deputy Commissioner
   e. Decide on re-entering FPP III on advice of Capitol Security Police (CSP)
   f. Ensure contact is maintained with the Police Officer

B. Specific parts and areas of FPP III

   1. Southside: Station 2. (In view of south door)

      a. Responsible Managers

Title	Organization	Names
Chief	Systems Development Bur. (SDB)	_____
Assistant Chief	SDB	_____
Staff Services Officer	SDB	_____

      b. Responsibility of Managers

         1) Ensure that employees:

            a) walk swiftly out of FPP III by a direct, but safe route, and move at least thirty yards from FPP III.
            b) avoid interference with any emergency work, but direct emergency crews to place of need.

         2) Control south area and employees
         3) Locate with south door in view
         4) Maintain contact with Chief, SPB
         5) Control access and use of south door and driveways on southwest and southeast

2. Eastside: Station 3. (In view of east door)

   a. Responsible Managers

Title	Organization	Names
Administrator	Systems Production Div. (SPD)	_____
Director, Data Center	SPD	_____
Mgr., Data Communications	SPD	_____
Mgr., Computer Operations	SPD	_____

   b. Responsibility of Managers

      1) Ensure that employees:

         a) walk swiftly out of FPP III by a direct, but safe route, and move at least thirty yards from FPP III.
         b) avoid interference with any emergency work, but direct emergency crews to place of need.

      2) Control of east area and employees
      3) Locate with east door in view
      4) Maintain contact with Chief, SPB
      5) Control access and use of east door and driveways on east and northeast

3. Contact, CSP: Station 4 (At east door or with the Police Officer)

   a. Assigned employee (one employee only)

Title	Organization	Names
Staff Member, Security	Technical Support Div. (TSD)	_____
Staff Member	TSD (backup)	_____
Staff Member	TSD (backup)	_____
Staff Member	TSD (backup)	_____

b. Responsibility of assigned employee

1) Maintain contact with the Police Officer, CSP, and other emergency units
2) Relay information; receive instructions from or to CSP and Chief, SPB
3) On departure from building, maintain contact with Chief, SPB

4. First Aid Teams:

a. Assigned employees

1) South: Station 5 (In view of south door)

Title	Organization	Names
First Aiders	SDB	_____
		_____
	SPB	_____
		_____

2) East: Station 6 (In veiw of east door)

First Aiders	SPD	_____
		_____
		_____
		_____

b. Duties of assigned employees

1) Assist with first aid as required and qualified
2) Maintain contact with door entrance guards, Section I.B.5., below

5. Door Entrance Guard

a. Assigned employees

1) South door (outside): Station 7

Title	Organization	Names
Staff Members	SMD	_____
		_____
		_____

2) East door (outside): Station 8

Staff Members	SMD	_____
		_____
		_____

b. Duties of assigned employees

1) Prevent entry of persons to building other than persons with emergency duties.
2) Relay information; receive instructions from or to CSP and Chief, SPB.

6. Alley Entrance Guard

a. Assigned employees

1) Southwest: Station 9

Title	Organization	Names
Staff Members	TSD	_____
		_____
Staff Members	Business Management Bur. (BMB) Mailroom Employees	_____
		_____

2) Northeast: Station 10

Staff Members SPD, Computer Operators _____

Staff Members _____

_____

b. Duties of assigned employees

1) Prevent entry of persons to alley other than persons with emergency duties
2) Mailroom employees

a) Exit FPP III through mailroom alley door (#196)
b) Close, but do not latch alley door
c) Clear alley of persons, vehicles and other movable equipment from mailroom south, when practicable.
d) Report significant events to Chief, SDB, or Chief, SPB

3) Computer room employees

a) Exit FPP III through computer room alley doors (#199) or from Forms Storage room alley door
b) Close, but do not latch, alley doors
c) Clear alley of persons, vehicles, and other movable equipment from computer room north, when practicable
d) Keep alley clear except for persons with emergency duties
e) Report significant events to Administrator, SPD; Chief, SDB; or Chief, SPB

7. Roof observer - from the hill north of FPP III

a. Assigned employees

1) West: Station 11 (from the hill north and west of FPP III)

Title	Organization	Names
Staff Members	SPD, Forms Handling	_____
		_____

2) East: Station 12 (from the hill north and east of FPP III)

Staff Members SPD, Forms Handling _____

_____

b. Duties of assigned employees

1) Exit FPP III through Forms Handling (#197) room alley door
2) Close, but do not latch, alley door
3) Clear alley of persons, vehicles and other movable equipment from Forms Handling room north, when practicable
4) Keep alley clear other than persons with emergency duties
5) Observe roof area from hill to north of FPP III
6) Report significant events to Administrator, SPD

8. Driveway Entrance Guard

a. Assigned employees

1) Southwest: Station 13

Title	Organization	Names
Staff Members	SDB	_____
		_____
		_____

2) Southeast: Station 14

Staff Members	SDB	_____
		_____
		_____

3) East: Station 15

Staff Members	SPD	_____
		_____
		_____

4) Northeast: Station 16

Staff Members	SPD	_____
		_____
		_____

b. Duties of assigned employees

- Ensure vehicles, other than emergency vehicles; do not enter FPP III parking area.

9. Other employees

a. South: Station 17 (area to south of FPP III) SDB

1) Walk swiftly out of FPP III by a direct, but safe route, and move at least thirty yards from FPP III.
2) Avoid interference with any emergency work, but direct emergency crews to place of need.
3) Remain in area #17 (in area of St. Edward's Drive), or other area as directed by managers.
4) Maintain contact with supervisors for information and instructions during work period.

b. East: Station 18 (area to east of FPP III) SPB

1) Walk swiftly out of FPP III by a direct, but safe route, and move at least thirty yards from FPP III.
2) Avoid interference with any emergency work, but direct emergency crews to place of need.
3) Remain in area #18 of frontage road, or other area as directed by managers.
4) Maintain contact with supervisors for information and instructions during work period.

10. Other managers and supervisors

a. Remain in appointed areas outside FPP III.
b. Maintain contact with division administrators and bureau chiefs.
c. Relay information and instructions as appropriate, to and from employees and managers.
d. Assist employees, in protection of State property and in the execution of this plan as appropriate.

11. All persons

Follow all safety precautions and stay away from areas of danger.

Section II. This section applies to a building evacuation from 5 PM to 8 AM, regular work days and weekends and holidays. (See Diagram, Schematic attached.)

1. FPP III and surrounding area

   A. Responsible manager

      1. Shift Supervisor, Computer Operations, SPD.
      2. Other managers and supervisors who may be in the area.

   B. Responsibility of manager(s) and other employees

      1. Control of all FPP III and employees.
      2. Ensure clearance of all employees from work areas.
      3. Ensure employees move to grassy area to east of FPP III near frontage road, IH 35, and remain at least thirty yards away from FPP III during an emergency (Station "A").
      4. Maintain contact with Police Officer and employees at assigned stations.
      5. Report status to Administrator, SPD, or Chief, SPB, as appropriate and when practicable.
      6. Assist with first aid as needed and if qualified.
      7. When practicable, based on numbers and capability of male employees present:

         a) Ensure protection of female employees.
         b) Ensure that employees assigned duty stations direct emergency vehicles to place of need.
         c) Prevent vehicles other than emergency vehicles from entering into parking area of FPP III.
         d) Assign an employee to each station as follows: All employees assigned stations, report to shift supervisor significant occurrences.

            1) Station "B": East drive; maintain contact with employees at Station "C" near southeast drive and at Station "E" at northeast drive.
            2) Station "C": Southeast drive; maintain contact with employees at Station "D" near southwest drive.
            3) Station "D": Southwest drive; assure clearance of alley on west side.
            4) Station "E": Northeast drive; maintain contact with employees at Station "F" near electric pole on high ground to north of FPP III.
            5) Station "F": Near electric pole on hill to north of FPP III;

               a) Ensure clearance of alley on north side of FPP III.
               b) Observe area to north of FPP III.

Section III. This section summarizes duties of the Police Officer during an emergency evacuation of FPP III.

1. Set off the fire alarms to cause evacuation of FPP III as shown in Physical Security Procedures, Section 8.B.1.d.1).
2. Telephone as appropriate,

   a. The Austin Fire Department, 476-4333
   b. The EMS, 474-1911
   c. The Capitol Security Police, Operations Deck, 475-2208

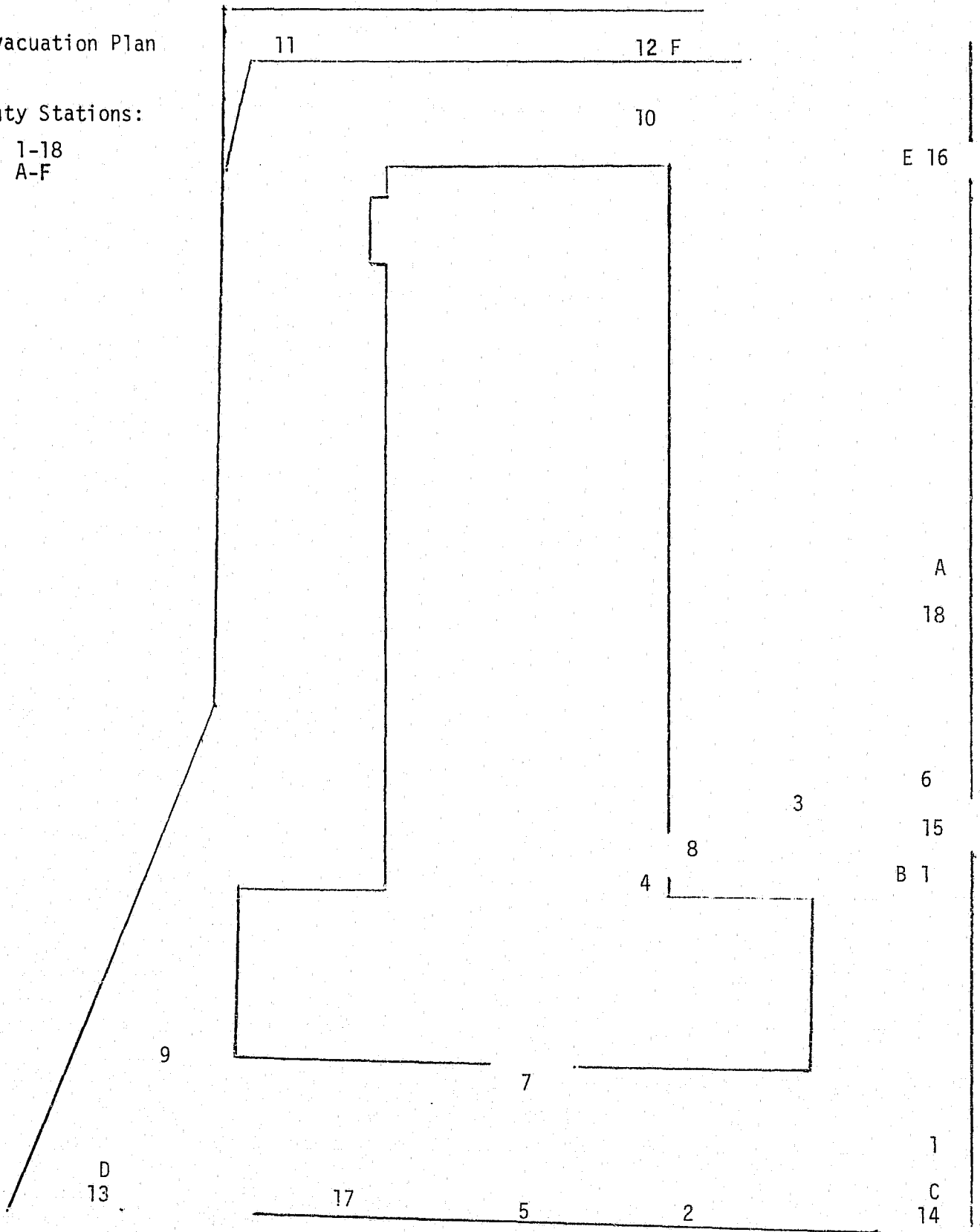
3. Release door monitor on alley doors.
4. Direct emergency crews to place of need.
5. Assist employees departing FPP III.
6. Assist in protection of State property.
7. Keep CSP contact employee informed of the situation. (See Section 1.B.3, Attachment S-3 above)

FPP III - DIAGRAM, SCHEMATIC

Evacuation Plan

Duty Stations:

1-18
A-F



TDHR, FPP III,
PSP, 3-79

RECAPITULATION: Designation of Stations

A. Regular Weekday Work Hours, 8:00 AM-5:00 PM

Station #	Location	Managers/Employees
1	East or South of FPP III	Chief, SPB, et al
2	Southside	Chief, SDB, et al
3	Eastside	Adm'r SPD, et al
4	East door, inside	Security Staff Member
5	In view of South door	First Aiders
6	In view of East door	First Aiders
7	South door, outside	Staff Members, SMD
8	East door, outside	Staff Members, SMD
9	Alley entrance, Southwest	Staff Members, TSD
10	Alley entrance, Northeast	Staff Members, SPB
11	Roof observer, Northwest	Staff Members, SPB
12	Roof observer, Northeast	Staff Members, SPB
13	Driveway, Entrance Guard, Southwest	Staff Members, SDB
14	Driveway, Entrance Guard, Southeast	Staff Members, SDB
15	Driveway, Entrance Guard, East	Staff Members, SPB
16	Driveway, Entrance Guard, Northeast	Staff Members, SPB
17	Area South of FPP III	Other employee, SPB&SDB
18	Area East of FPP III	Other employee, SPD

B. Weekends, holidays, and regular work days 5:00 PM-8:00 AM

A	Area East of FPP III	Staff Members, SPD
B	Area East of FPP III	Staff Members, SPD
C	Driveway, Southeast	Staff Members, SPD
D	Driveway, Southwest	Staff Members, SPD
E	Driveway, Northeast	Staff Members, SPD
F	Roof observer, North	Staff Members, SPD

MEMORANDUM

TEXAS DEPARTMENT OF HUMAN RESOURCES

SUBJECT: Physical Security Procedures, Revision #7

TO:

Mr. Richard E. Reich
Administrator
Systems Production Division
State Office 854-0

FROM:

Dean L. Jessen
Chief
Systems Processing Bureau
State Office 850-0

DATE: March 19, 1979

The Physical Security Procedures, Data Center, FPP III, Revision #7, is hereby published and is effective on receipt.

Make the following changes for this revision which are marked, "TDHR, FPP III, PSP, 3-79", in the lower right corner of each page.

Add page RR-1, Record of Revision, after the title page and before TC-1, Table of Contents (Remove the presently used Record of Revisions page). This page shows the record of revisions made in the Physical Security Procedures edition of April 1978. The person inserting the pages of this revision should initial in the column for that purpose.

Replace page 1.2. This page changes the title of the "Security Guard" to "Police Officer" in Section 1.C.4.a.

Replace page 1.3. This page changes the title of the "Security Guard" to "Police Officer" in Section 1.C.4.b. and c.

Replace page 1.4. This page changes the title of the "Security Guard" to "Police Officer" in Section 1.E.

Note: Additional changes from the title "Security Guard" to "Police Officer" will be made, on pages where this title occurs, as other revisions are necessitated.

Replace page 4.3. This change, in Section 4.B.1.c., clarifies records maintained for issuance of a Data Center Security Badge.

Replace page 4.3.1. This page receives overflow from the addition made on page 4.3.

Replace page 4.4. This page corrects a transposed letter in a word in Section 4.D.1.

Replace page 4.7. This page eliminates a telephone number in Section 4.I.3. which is no longer in use.

Replace page 4.8. This page, in Section 4.J.3., authorizes the opening of the Producton Control area during regular day work hours to persons who are otherwise authorized entry into the Data Center.

Replace page 8.1. This page corrects a letter in a word in Section 8.A.3.b.

Replace page 8.2. This page in Section 8.A.3.e.2)b)., provides for a smoking (break) area in the Forms Handling room, 197.

Replace page 9.2. This page corrects a letter in a word in Section 9.F.4.a.

Replace page A (Attachments). This page updates the list of attachments with this revision to include Attachment "S", "Plan for Evacuation of FPP III".

Replace Attachment "K", page 1 and 2, with Attachments "K-1", "K-2", "K-3", and "K-4". These pages update the "Procedure for Power Cutoff of the Data Processing and Terminal Equipment".

Replace Attachment "L". This attachment updates the list of "FPP III Employees with Training in Emergency Medical Treatment Procedures".

Replace Attachment "Q". This attachment updates list of employees home telephone number, "Emergency Contacts and Notifications".

Add Attachment "S". This attachment establishes the "Plan for Evacuation of FPP III".

The changed part of each page is shown by a vertical line in the left margin.

File this memorandum behind the last page of subject manual.

Dean L. Jessen

DLJ:JLB:MN

Attachments (11 copies to addressee)

cc: Ms. Mary Awbrey, 810-0 (6 copies of attachment)
Mr. L. D. England, 800-0
Mr. John C. Musgrove, 800-0
Mr. John H. Windham, 800-0
Ms. Sherron E. Heinemann, 800-0
Mr. David Kellogg, 820-0
Mr. Bill Stobie, 851-0
Mr. Harold K. Dudley, 440-0
Mr. John H. Heir, 461-0
Mr. Homero Rodriquez, 700-0
Mr. Jack Blanton, 000-0
Mr. William S. Wood, 150-0
Mr. Marlin W. Johnston, 200-0
Mr. Edward L. Richards, 250-0
Ms. Hazel S. Baylor, 300-0
Mr. Wesley L. Hjornevik, 400-0
Mr. Merle S. Springer, 500-0
Dr. E. W. Greif, 600-0