LAW ENFORCEMENT ASSISTANCE ADMINISTRATION (LEAA)

POLICE TECHNICAL ASSISTANCE REPORT

SUBJECT:	Computer Security Requirements Study
REPORT NUMBER:	77-0[illegible]124
FOR:	State of Nevada Computer Facility
CONTRACTOR:	Public Administration Service 1776 Massachusetts Avenue, N.W. Washington, D. C. 20036
CONSULTANT:	Richard L. Goheen
CONTRACT NUMBER:	J-LEAA-002-76
DATE:	March 31, 1977

Table of Contents

FOREWORD

This report was prepared in response to a request for technical assistance from the State of Nevade Computer Facility in doing a computer security requirements study. The consultant assigned was Richard L. Goheen, and other personnel involved in processing the request were:

Requesting Agency:	Mr. Arthur F. Crosby Director, Computer Facility State of Nevada
State Planning Agency:	Mr. Harry A. Lipparelli Acting Chief, Planning & Training Division Department of Law Enforcement Assistance State of Nevada
Approving Agency:	Mr. Gwen M. Monroe Director, Program Development & Assistance Division LEAA Region IX (San Francisco)

I. INTRODUCTION

The State of Nevada Computer Facility in Carson City, Nevada, is seeking technical assistance to assure its physical security against threats to the computer from arsonists and terrorists as well as from persons who are capable of manipulating the software or jamming the computer operations. In addition to advice on security for its building, the facility also desires security training for its personnel against forced entry, bomb threats, civil disturbances, and other threats to property as well as training in storing criminal justice data.

The Nevada Computer Facility comes under the general supervision of the Data Processing Commission, which is the main user of the facility. The Commission is chaired by the State Comptroller, an elected official; all other members are career civil servants. As a service bureau operation that provides a data processing capability for tasks that are designed and programmed by the users, the Facility is used mainly for processing operations, although there is some data base management, most of which is confined to automobile registrations and driving permits. The facility also has an on-line capability, with terminals in several locations throughout the state.

It is a 24-hour a day, 7-days a-week operation. During nighttime hours (about 5 p.m. to 7 a.m.) and on weekends, it is often manned by one computer operator per shift.

The facility contains two main frames, an IBM 370-158 and an IBM 370-145, disk and tape drives, and printers. It is situated at 501 E. Third Street, Carson City, and employs 27 persons.

The value of the computer hardware owned by the facility is $2.3 million; that of the software, is between $10 and 20 million.

The following persons were interviewed during the on-site phase of this assignment:

Mr. Arthur Crosby
Director
Computer Facility
State of Nevada

Mr. Michael Meizel
Chief, Buildings and Ground Division
Department of General Services
State of Nevada

Mr. John Peevers
Chief, Communications and Identification Division
Department of Law Enforcement Assistance
State of Nevada

Mr. Pete Rasner
Sheriff
Carson City, Nevada

II. UNDERSTANDING THE PROBLEM

This assignment is a security survey. Generally, such surveys consist of threat identification, probability estimates of their occurrence, the likely damage (in dollars) that would ensue, examination of the current security posture, and recommendations for a cost-effective program to offset the probable annual losses. In addition, such a survey would include an examination of the facility's contingency planning for emergencies, back-up operations, and disaster recovery.

During the consultant's initial meeting with the facility's Director, Mr. Arthur F. Crosby, he explained that the State of Nevada Data Processing Commission had requested $20,000 from the state legislature to increase the physical security of the computer site. That request is expected to be approved during the current legislative session. It will have an even better chance of obtaining approval, he said, if a copy of this report is made available to the legislature.

The director expressed considerable concern about the vulnerability of the Computer Facility building to attack by terrorists and demonstrators. Since there was no request to inquire into the validity of the $20,000 figure (that is, a threat analysis) or to evaluate the facility's defenses against employee attack, the survey is confined to evaluating defenses against outside physical attack.

The survey does not address the possibility of data manipulation by outsiders, which was alluded to in the requesting letter of transmittal. That would require a detailed examination of the facility's communications network and operating system, which in turn would necessitate several month's effort and the assistance of competent technicians.

Also, the survey included no provision for training of employees in security. It was explained to Mr. Crosby that "training" in these matters could be given by himself. What the facility needs are written procedures covering certain situations. The survey attempts to learn what those potential situations are and what procedures are needed to deal with them.

The survey addresses only in part the most serious security weakness of the facility — the almost total lack of contingency planning. The facility has no back-up machine capability. It has an agreement with the State of Utah to use its hardware if the facility's own were to be destroyed or severely damaged, but that agreement is virtually worthless. Not only is the Utah facility running full-time with its own operations, but the on-line operations of the Nevada facility cannot be switched elsewhere. Theoretically, the most important 10 to 15 per cent of the Nevada facility's operations could be processed in Utah without impacting on the accomplishment of the latter's mission. That, however, would require a great deal of detailed planning and inquiries into such matters as compatibility of the software operating systems and assembly programs.

Furthermore, although the facility keeps grandfather copies of its tapes stored off-site, it has no copies of the system documentation so stored.

Currently, State of Nevada auditors are examining the facility. They plan to deal with the contingency planning in detail.

Contingency planning is an important part of a security program. It acts as a second line of defense if preventive measures fail and also reduces the cost of those measures. There is less incentive, then, for investing in a fortress-like security program.

Given, however, the absence of such planning and its likely continuation for some time, the present survey must concentrate on measures that will, within reasonable costs, protect against any foreseeable threat posed by terrorists, saboteurs, or demonstrators.

III. ANALYSIS OF THE PROBLEM

The Community Setting

The Nevada Computer Facility is situated in a neighborhood of other state-owned buildings and private residences. To the north and west are state-owned facilities; to the east is a school and single-family houses beyond; and to the south, a residential area. A block to the south are several cottages that, together, comprise an orphanage. Juveniles from the orphanage, it is suspected by facility personnel, have caused several acts of minor vandalism to the facility and to the automobiles belonging to its employees.

Current Security Measures

Building Exterior

The facility is contained within its own one-story building that is constructed of prefabricated, reinforced-concrete slab. The roof is of the same construction. There are seven openings in the walls: five are doors, including the main entrance on the north side, three entrances on the south, and one on the west. The south side also contains a six-by-three-feet blow-out panel placed as a pressure release in case of a boiler explosion. There is also an opening for the radiator of the diesel generator that acts as an alternative power source for the facility.

A step-down transformer that comprises an element of the facility's power distribution system sits, protected by a metal container, on the southwest corner of the facility grounds.

Chilling units for the facility's two air conditioning systems are on the roof of the building.

Lights are provided over each building entrance. All but one are activated by solar switches. There are a number of light standards around the parking lot west of the facility, but in the interests of energy conservation, these have not been turned on for some time.

Building Entrances

The main (north) entrance is constructed of metal stile-and-rail doors, the panels of which are Underwriters Laboratories approved burglary-resistant glass. There are floor-to-ceiling windows, approximately four feet wide, on either side of the doors. They are also of burglary-resistant glass. The doors are equipped with pin tumbler mortise lock sets that are operated by keys on the exterior side and panic bars on the interior. The locking device is a spring latch. The exterior cylinder is protected by a cylinder guard.

Inside the main entrance is a glass-enclosed foyer. To the right, behind the glass wall, is the receptionists' office; behind the wall to the left is another office. The front contains a second set of double doors constructed of metal stiles and rails and tempered glass panels. The doors are operated by

an electric strike, the control to which is in the receptionists' office. A second control button is near the console in the computer room.

The west side door is similar in construction and configuration to the main entrance except that there are no windows beside the exterior doors and the right and left foyer walls are of masonry, not glass.

The three south end doors are similar: metal clad, hollow double doors. The inactive leaf is held in place by aluminum flush bolts at head and foot that are activated by a lever set in the leaf edge. The active leaf is equipped with look sets consisting of key-in-the-knob cylinders and dead latches.

Key Control

All exterior locks are keyed alike. That is, one key can unlock them all. Most locks to interior doors are also keyed alike but require a key different from that for exterior locks. Keys are controlled by one of the two receptionists, Viola Jewett. Two keys, one for exterior locks and another for interior, are issued to all employees. They must receipt for them. The keys are imprinted with the words, "Do Not Duplicate." Twice in the recent past, after the termination of an employee, all exterior locks were changed.

Computer Room

The computer room occupies the center of the building and is bordered by offices or corridors on the north, east, and west sides. The south side of the computer room opens directly onto the building exterior. (It is the only south end entrance equipped with panic bars.) The north end of the computer room is constructed of metal and glass walls, the remaining walls are of sheet rock.

The room has nine entrances, only one of which--the exterior door--is kept locked. Three of them open into offices and one into a store room. The others open to the building exterior or, either directly or indirectly, into corridors. All doors are equipped with pin-tumbler, mortise locksets.

Visitor Control

In addition to employees, facility users have unquestioned access to the building. Those entering through the main entrance are admitted when the receptionists press the control button for the electric strike. In the southeast corner of the building is a room ("bursting room") containing machinery employed by EDP users to burst checks and decollate printouts. Admission to this room is through one of the southside entrances, which is also used for making deliveries to the facility. The door is kept locked. Anyone seeking admittance either to the bursting room or to make deliveries must summon computer room personnel by means of a door bell button placed beside the entrance. At least one regular user of the bursting room has been known to place tape across the door's deadlatch so as to keep it retracted and, thus, permit the user free access through the entrance.

During nighttime hours, any person other than an employee, who desires to enter the facility must use a door bell to summon the computer operator. Door bells are placed at the main entrance and at the one near the bursting room. The active leaf of the latter door is equipped with a peephole. There is also an overhead fluorescent lamp so that callers can be identified through the peephole during hours of darkness.

Persons other than employees or users are considered visitors. Visitors are admitted by the receptionists only if they have an appointment, of which the receptionists are notified in advance, or by specific permission of facility executives. Visitors are not required to sign in. The identification required of them is a business card.

The outside doors at the main entrance are open from 8 a.m. to 5 p.m., Monday through Friday. A stranger may therefore enter the facility as far as the foyer. When that occurs, one of the receptionists goes to the inside door, opens it, and asks the stranger's business. More often than not the stranger wants only directions to some other building. If the stranger has an appointment with someone in the facility, he is admitted.

All persons entering the facility between 5 p.m. and 7 a.m. are required to complete a log. It contains space for the person's name and agency, time in, and time out. Persons admitted during these hours are employees, user agency personnel, and IBM customer engineers.

Security and Police Protection

Security and police protection are provided by the Capitol Security Force and the Carson City Sheriff's Department.

The Capitol Security Force is an element of the Division of Buildings and Grounds, Department of General Services, State of Nevada. The force presently consists of six security officers and one watchman. (The watchman position is not exclusively concerned with security; the person occupying it may also perform custodial duties.)

The mission of the Security Force is to protect the State Capitol, the State Assembly Building (when the legislature is in session) and about 20 other state-owned and leased buildings in Carson City. The force mans two posts: an around-the-clock fixed post at the Capitol; and a seven-days-a-week, midnight-to-8 a.m. roving post that covers the remainder of the buildings. There is, thus, no security force protection of the Computer Facility during daylight hours or from 4 p.m. to midnight.

The Carson City Sheriff's Department has 50 sworn officers and 2 clerks. Its headquarters is three blocks from the Computer Facility. There are five patrol beats within the city, with one officer assigned to each during all hours. When asked how often these patrols take an officer past the Computer Facility, Sheriff Rasner said his officers' time was taken up with answering calls for service and they had little time for preventive patrol.

He was aware, however, of the importance of the Computer Facility. He said it was in a primary response category: officers would be pulled off

lower priority calls to respond to a call from the facility. The Sheriff said his officers could respond within two or three minutes. He also agreed to the Department's Communications Center monitoring any alarms that may be installed in the Computer Facility. Sheriff Rasner also said he had within his department two trained bomb disposal technicians and a seven-man special weapons and tactics team.

In the event of a civil disturbance or demonstration at the facility, he said he could dispatch 90 men to it within 20 minutes: 50 sworn policemen, 20 police reserves, and 20 members of the Sheriff's Posse. He said he could not recall a civil disturbance that had occurred in Carson City.

Additional Police Protection

Mr. John Peevers of the Department of Law Enforcement Assistance, State of Nevada, said he could not imagine a civil disturbance in Carson City about which he would have no advance warning. The city contains no radical groups, and there is a very low probability that spontaneous disorders would occur such as those in some urban areas following Dr. Martin Luther King's death.

There is an American Indian community four or five miles south of the city. Mr. Peevers has heard that the American Indian Movement, a sometimes violent group concerned with Indian rights, has recently been active in that community. He is uncertain, however, about the success of its efforts.

Mr. Peevers said that if a civil disorder occurred in the vicinity of the Computer Facility, sworn officers of his Department as well as 20 to 30 members of the Nevada Highway Patrol could respond within 20 minutes. He also revealed that the Department had a bomb technician and had developed a model bomb threat plan that would soon be issued to all state agencies.

Vulnerability

Theoretically, terrorists or demonstrators could disable the Computer Facility through either of two means: preventing facility employees from reporting to work, or damaging some element critical to the facility's operation.

Preventing employees getting to work is an extremely remote threat. There are sufficient law enforcement officers in Carson City to control any but the largest civil disorders or demonstrations. A planned demonstration of the necessary size would be known to state and county officials far enough in advance of the event that the proper countermeasures could be taken.

On the other hand, if a group of terrorists or saboteurs chose to inflict damage on the facility that would interrupt operations, it could succeed. There are a number of security weaknesses at the building, which break down into three categories: physical, procedural, and exterior.

Physical Weaknesses

All exterior doors at the facility are vulnerable to defeat by semiskilled physical attack. The outer doors at the north and west entrances are secured by spring latches that can probably be defeated by shove knives or any other instrument of strong flexible material. During an experiment with one leaf open, the latch on the other leaf of the north end exterior door was easily defeated by a pen knife. An attempt was then made with both leaves closed to defeat the latch with a hacksaw blade. Although contact with the latch was made, the blade was not of sufficient bulk to spring it. Nevertheless, the suspicion remains that the failure was due more to the security of the door assembly. The same can be said about the west-side door.

The three south-side doors contain key-in-the-knob locks that are vulnerable to very rapid defeat by wrenching techniques or by removing the lock cylinders with a dent puller. Moreover, the doors are so flimsily constructed that they often do not close properly. It is therefore possible that an intruder would be able to open those doors without using any force.

The interior double doors at the main entrance can be defeated (and have been at least once in the past) merely by pulling on the active leaf with some force.

The second physical weakness comprises the glass wall and doors in the north-side foyer and the glass door in the west-side foyer. In either case, a person standing outside the building has a clear view of the computer room. Any saboteur wishing to "case" the facility for the possibility of inflicting later damage or determining when a nighttime computer operator has left the computer room can do either without having to enter the building.

The third physical weakness is the absence of any means other than the telephone for summoning help in an emergency. There are situations when the telephone is much too slow, demanding time to dial, time waiting for the call to be answered, and time to explain why the call was made. A second problem is the relative case with which the telephone lines can be severed.

The final weakness in this category is the blow-out panel on the south wall. It covers an opening large enough for a man to walk through and could probably be removed in seconds by attaching one end of a cable to it and the other to a motor vehicle.

Procedural Weaknesses

The most serious weakness in this category is the poor visitor control procedures. A receptionist opening inner doors to a stranger can be overpowered or intimidated, as can a computer operator alone in the building at night. Permitting users to enter the building at night through the Bursting Room entrance is an unnecessary sacrifice of security to convenience. Failure to register all visitors eliminates the possibility of a sometimes valuable investigative trail when otherwise unexplainable incidents occur later on.

Key control procedures at the facility are deficient in two respects. Key-controlled locks on exterior doors, for which keys are issued to all

personnel increase the possibility of misuse. Keys can be lost, stolen, or duplicated. The second deficiency is that of making it possible for all exterior doors to be unlocked from the outside. Each such door only increases the probability of successful violation of perimeter security.

The third procedural weakness is the failure to lock all computer room doors during night and weekend hours. A person forcing his way beyond the perimeter barriers would be in the computer room before the operator had time to summon help.

Exterior Weaknesses

There are two weaknesses in this category: the transformer/generator and the air conditioning chillers. All three units are on the exterior of the building or can be attacked from the exterior. Damage to the chillers or to the transformer and generator will disable the computer facility. To protect them from possible attack would involve very costly construction.

IV. FINDINGS AND CONCLUSIONS

General Assessment

A group of terrorists or saboteurs attacking the facility could inflict the most severe damage by destroying the computer software and system documentation. It would take far longer to recover from that kind of attack than from any other. That is especially true with respect to the documentation, since no other copies of it exist.

The second most critical element is the computer hardware. The facility has no back-up machine capability. Destruction of or serious damage to it would entail an interruption of a duration equal to the time required to replace or repair the equipment. Although equipment manufacturers have in the past gone to great lengths in quickly replacing destroyed hardware, there is never a guarantee that they can do so in every case.

Since the Computer Facility has no comprehensive contingency plans or back-up hardware, it is most important that extraordinary measures be taken to prevent a successful attack upon the software and equipment, all of which is stored within the computer room. Means of doing that are discussed below under the heading Preventive Measures.

Less serious is the destruction of or damage to the air conditioning chillers, or transformer and generator. An attack upon them can, indeed, interrupt EDP operations, but these items are not as costly to replace. The transformer/generator, moreover, presents something of an inherent security barrier. Someone wishing to disable the facility by interrupting the power supply would have to know that 1) destruction of the transformer by itself is not enough to cause such interruption, 2) an auxiliary generator exists, and 3) a large grill on the south wall conceals the radiator of that generator. On the other hand, someone possessing that information could very easily disable the generator by punching with a sharp object, through the grill and into the radiator.

Successful attacks against the chillers or the transformer/generator cannot be prevented without extensive and costly construction. That being the case, the only remedy left is contingency planning, which is discussed in the section entitled Damage Reduction Measures.

Preventive Measures

A security system established to prevent a successful attack by humans is ultimately dependent upon the arrival or presence of a trained armed force large enough to control an attempted penetration. The armed force forms one the three elements of a reliable security system. The others are physical and procedural barriers that delay attackers but allow authorized persons to pass through and a means of notifying the response force that the protected area is under attack.

The only possible response force is the Carson City Sheriff's Department. The Capitol Security Force is too small to be a factor. Although there was no way of testing the assumption, it is supposed that the Sheriff's Department would furnish a force rapidly enough and large enough to prevent all but minor damage to the facility by terrorists. That is possible, however, only it changes are made in the physical barriers and procedures. Otherwise, terrorists can now cut the facility's telephone lines and quickly enter the building to the computer room and inflict damage, almost at their leisure.

To prevent that, the building perimeter entrances must be modified, the key control and visitor control procedures must be changed, and alternate, rapid means of notifying the Sheriff's Department must be installed.

The recommendations that follow are elements of a system whose ultimate goal is to allow receptionists or computer operators time to notify the Sheriff's Department of an attack against the facility before the attackers can significantly damage computer hardware or software.

To accomplish that the recommendations seek to achieve these five subgoals:

1. To prevent any attack against the south and west doors except those whose success entails the creation of a level of noise that would be unacceptable to most potential attackers or, allowing for attackers who will risk making excessive noise, back up the physical barriers with an alarm system that will immediately notify the Carson City Sheriff's Department if the doors are opened or the south-end blow-out panel removed.

2. To prevent potential attackers from being able to observe what facility personnel are doing at any particular moment.

3. To prevent the defeat of perimeter security through the use of illegally or fraudulently obtained keys by eliminating all key-operated exterior locks.

4. To prevent entry gained through the overpowering or intimidation of receptionists or computer operators by keeping a barrier between the person seeking access and the facility interior until the receptionist or computer operator is assured of the person's identity and that of other persons, remaining concealed until the interior door is opened, in order to gain "piggy back" entry along with the person having authorized access.

5. To provide reliable means for rapidly notifying the Sheriff's Department of attacks or possible attacks against the facility.

Damage Reduction Measures

Since successful attacks on the chillers and transformer/generator cannot, given their present configuration, be prevented, it is important that certain steps be taken to reduce the amount of down time that would result from a successful attack. Those actions would include assessment of likely damage, repair provisions, liaison with suppliers and manufacturers, pre-

paration for procurement, and the acquisition of spare parts. The idea is to accomplish now as much as possible of the work that would have to be done if these units were destroyed.

V. RECOMMENDATIONS

1. Replace the three south-end exterior doors with door assemblies meeting the specifications prescribed in Appendix A.

2. Replace the double glass doors in the north- and west-end foyers with single swinging door assemblies meeting the specifications prescribed in Appendix A.

3. Install locking systems on the exterior doors of the north and west entrances that meet the specifications prescribed in Appendix B.

4. Install a buzzer-reply intercom system next to the exterior door at the main entrance that meets the specifications prescribed in Appendix C.

5. Install in the north-end foyer a closed circuit television (CCTV) system that meets the following requirements:

   a. The camera is placed so that it affords a view of the entire area of the active leaf of the exterior door.

   b. The camera is enclosed in sturdy, dust-proof housings that are installed with tamper-proof connectors.

   c. The level of the lighting in the foyer is raised as necessary to permit a video image of adequate quality.

   d. The receiver for the CCTV system is in the vicinity of the computer console and affords an image comparable to that of a conventional television receiver.

6. Replace the tempered glass wall in the north-end foyer with one constructed of 2x4's (either metal or wood spaced 16 inches apart on center) and wall board on each side of the framing.

7. Install balanced magnetic contact switches on both levels of all exterior doors, including the single door leading to the roof, that will transmit a signal directly to the communications center in the Sheriff's Department headquarters building. The transmission line should have a supervisory circuit that will sound an alarm if the line is cut or if the system is malfunctioning. The transmission line and supervisory circuit should have, in case of electrical power failure, an auxiliary power source that will ensure at least 48 hours of continuous service. The system is to consist of two key-activiated subsystems: one for the three south-end doors, the blow-out panel (see recommendation 9), the roof door, and the west end door. The other system should be dedicated to the north-end entrance should be activated only in the event the building is left

unoccupied for a period of time. The other system is to be activated each workday evening to be determined by the Facility Director.

8. Install a taut-wire device across the interior side of the blow-out panel on the south side of such tension and volume as to detect attempts to remove the panel or cut through it.

9. Install distress alarms near the computer console and in the receptionists' office that will transmit a signal directly to the communications center in the Sheriff's Department headquarters. It should use transmission lines similar to those specified for the anti-intrusion alarms described in Recommendation 7.

10. Adopt key control procedures that will prohibit the permanent issue of keys to any employees other than a few high-ranking staff members and that will provide a set of interior door keys maintained within the computer room.

11. Adopt access control procedures substantially similar to those prescribed in Appendix D.

12. Coordinate alarm system and emergency response procedures with the Sheriff's Department to include, if possible, periodic tests.

13. Devise a contingency plan for damage to the air conditioning chillers, transformer, and generator that includes the following elements:

    a. Liaison with equipment manufacturers to arrange rapid supply of needed spare parts.

    b. Liaison with the Buildings and Grounds Division or local contractors to ensure that needed mechanics are available in case of emergency.

    c. Prepared procurement documents that can be used immediately after the damage is known.

    d. A contingency fund based upon an assessment of likely repair costs.

    e. A spare radiator for the emergency generator on hand at the computer facility

APPENDIX A

Door Assembly Standards
I. South-End Entrances

1. Door Type and Construction. Flush type, outward swinging, double doors of 24-gauge sheet metal bounded to a nonresinous kiln-dried wood interior at least 1 3/4 inches thick. Clearance between the two leaves of the door, when they are in the closed position, should not exceed 1/8 inch along the hinge and 1/4 inch at the top and bottom.

2. Door Frames. Door frames should be made of solid wood with a minimum thickness of two inches or of solid wood covered with sheet steel having a minimum thickness of 18-gauge. Clearance between the edge of the door and its pause, when the door is in its closed position, should not exceed 1/8 inch along the hinge and 1/4 inch at the top and bottom.

3. Locking Devices

   a. Neither leaf of the door should be capable of being unlocked or pulled open from the building exterior. That is, the doors should have no keyways, knobs, handles, or levers.

   b. The active leaf of the door should be fitted with a deadlatch with a minimum 5/8 inch throw that allows egress to the outside by operating a panic bar.

   c. The inactive leaf of the door should be fitted with hardened steel top and bottom flush bolts each having a minimum 3/4 inch throw. These bolts should be received by metal reinforced holes set into floors or door frames.

4. Protection of Strike. All doors should be so constructed as to have a piece of metal that covers the opening between both leaves of the door at the area of penetration of the deadlatch and that can deter the insertion of tools, thus preventing the exertion of pressure against the latch. The piece of metal shall be attached to the door with round-head carriage bolts or one-way screws.

5. Hinges. Door hinges should be fitted with nonremovable hinges.

6. Openings. Each door should be fitted, in the active leaf, with an optical door interviewer installed in a hole having a maximum area of 1/2 square inch, drilled or otherwise cut through the door. The optical door interviewer should be located midway between the leaf's two sides and approximately 4' 9" above floor level. The interviewer should be so designed and constructed that no bolts or screws are exposed on the outside of the door. The edges of the interviewer case should not exceed 1/4 square inch. This opening should be fitted with a system of optical lenses which provide a wide-angle view (minimum 90°) from inside the door and are securely fixed into the interviewer.

7. Door Closer. The active leaf of each door should be fitted with a door closing device capable of closing and latching the door no matter how far apart it may be.

II. North and West Ends Interior Entrances

1. Door Type and Construction. Flush type, outward swinging single doors of solid core wood construction at least 1 3/4 inches thick.

2. Door Frames. Door frames should be constructed as specified in paragraph 2 under Part I. above, or of hollow steel fabricated from sheet steel with a minimum thickness of 16-gauge provided the hollow space inside and behind the frame is filled with cement grout or a similar crush-resistant material for the entire space within 12 inches above and below the strike. Clearance between the edge of the door and its frame, when the door is in its closed position, should not exceed 1/8 inch along the hinge and lock sides and 1/4 inch along the hinge and lock sides and 1/4 inch at the top and bottom.

3. Locking Devices

   a. West-Side Door. The west-side interior door should be fitted with a deadlatch with a minimum 5/8 inch throw which allows egress to the outside by operating a panic bar. The deadlatch should be operable by key from outside the door. The lock cylinder should be protected by a cylinder guard.

   b. North-Side Door. The north-side interior door should meet the specifications for the west-side door. In addition, it should have an electric strike installed which can be operated by buzzers installed at the receptionists' desk and at the computer console.

4. Protection of Strike. The strike should be protected as prescribed in Paragraph 4 of Part I. above, except that the piece of metal should cover the opening between door and the frame.

5. Hinges. Door hinges should be fitted with nonremovable hinges.

6. Openings (West side door only). The door should be fitted with a vision panel constructed of underwriters laboratories approved burglary-resistant glass sufficiently large that a person inside the door will see any anyone in the foyer.

7. Door Closer. Each door should be fitted with a door-closing device as specified in Paragraph 7 of Part I. above.

APPENDIX B

Locking System
North and West Ends Exterior Doors

1. Locking Devices. The current spring latches on the north and west entrance exterior doors should be replaced with deadlatches.

2. Method of Opening. The north and west exterior doors should have installed electronic combination locks having electronic push buttons into which the entrant keys the combination to actuate an electric strike. Egress to be by means of panic bars. The strike must be capable of remote operation by buzzers placed at the computer console and the receptionists' area.

3. Signalling device (north and exterior door only). The strike should have installed a device that will cause both an antible and visual signal in the vicinity of the computer console when the strike is disengaged from the deadlatch and a different audible and visual signal when the strike is engaged with the deadlatch.

APPENDIX C

Buzzer - Reply Intercom System

A buzzer - reply intercom system should meet the following specifications:

1. Speakers installed at the following locations:

    a. Beside the exterior doors of the main entrance

    b. Inside the north-end foyer

    c. At the receptionist's desk

    d. At the computer console

    e. At the east end of the east-west corridor

    f. At the south end of the north-south corridor.

(The latter two speakers are required for those cases when someone seeks entry to the facility and the computer operator is out of the computer room.)

2. Voice clarity of the audio intercom system shall be at least as good as conventional telephone standards.

3. The hardware outside the main entrance should include recessed speakers and microphones as well as a vandal-resistant buzzer for signalling the computer operator or receptionist. All equipment should be installed so that it is protected from the weather.

APPENDIX D

Recommended Access Control Procedures

1. Daylight Hours

1.1 Definition. Daylight hours are defined as those hours during which the receptionists are normally on duty.

1.2. Access through the main Entrance

1.2.1. Employees. Facility and authorized user agency employees and IBM customer engineers should be granted unquestioned access to the building. User agencies should submit, in two copies, a list of all employees authorized access to the facility. One list should be maintained in the receptionists' area and another at the computer console. User agencies are also responsible for notifying the Facility Director immediately of any employee whose employment is terminated or who, for any other reason, is no longer authorized access to the facility.

1.2.2. Method of entry. Facility employees, authorized user agency employees, and IBM customer engineers should be admitted when the receptionists open the interior main entrance door by retracting the electric strike.

1.2.3. Visitors. The following procedures should be adhered to upon the appearance of a stranger within the main entrance foyer.

1.2.3.1. The receptionist should, by means of the intercom system, learn the stranger's business.

1.2.3.2. If the stranger has an appointment within the facility and the receptionist is aware of that appointment, the visitor should be required to display a driver's license and sign the visitor's log before being admitted to the building.

1.2.3.3. If the stranger has no appointment (or has one of which the receptionist has no prior knowledge) and wishes to see a specific person in the facility, that person should be called to the reception area. If he or she approves the visitor's entry, the visitor should be required to display a driver's license and sign the visitor's log.

1.2.4. Information seekers. All persons who do not wish to enter the facility but are seeking information or directions should be spoken to only through the intercom system.

1.2.5. Emergencies. In case a person seeks entry after being denied it, attempts to intimidate the receptionist through the glass wall, or rushes into the facility behind someone granted authorized entry, the receptionist should activate the distress alarm con-

nected to the Sheriff's Department.

1.3. Access through the loading dock door

1.3.1. Deliveries. All persons making deliveries should be required to first report to the north entrance where the receptionist should learn what they are delivering and require them to sign in the visitor's log. If the delivery is in any way suspect, the receptionist should call the Facility Director or his representative. If the delivery is legitimate, the receptionist should, through the intercom, notify computer room personnel that they may open the loading dock door.

1.3.2. User Agency personnel. All authorized user agency personnel seeking to use bursting room facilities should be admitted through the loading dock door by computer room personnel.

1.3.3. Precautions. Whenever the loading dock door bell is sounded, computer room personnel should, before opening the door, observe who the person is through the optical door interviewer. If the employee does not recognize the person or sees no one, the door should not be opened.

2. Nighttime Hours

2.1. Definition. Nighttime hours are defined as those hours during which access to the facility is controlled by computer room personnel.

2.2. Authorized access

2.2.1. During nighttime hours only facility employees, employees of users agencies, and computer hardware service personnel should be admitted to the facility. All persons admitted should be admitted only through the main entrance. The loading dock door should not be used to admit persons to the building during nighttime hours.

2.2.2. Employees needing to enter the facility will open the exterior door using the electronic combination lock. When the strike is retracted, an alarm will sound in the computer room. The computer room employee should observe the person or persons entering on the CCTV monitor. When the exterior door closes and the lock is engaged, a second signal will sound in the computer room.

2.2.3. If the computer room employee recognizes all persons who entered the exterior door as those authorized entry into the facility and he has received the signal showing the exterior lock to be engaged, he should activate the electric strike on the interior door to admit those persons.

2.2.4. If he does not receive the signal that the exterior door lock is engaged he should through the intercom system, request the person in the foyer to pull on the outer door until the lock is engaged.

If the person in the foyer appears hesitant, frightened, or otherwise under duress, the computer room employee should activate the distress alarm connected to the Sheriff's Department.

2.2.5. If there is a combination of authorized persons and persons whom the computer room employee does not recognize in the foyer, he should, through the intercom system, inform all parties that the door will not be opened until the unauthorized persons have gone. If those persons leave and the computer room employee receives the signal that the outer door lock is engaged, he should activate the electric strike on the interior door to admit the authorized persons. If the authorized persons refuse to leave, the computer room employee should activate the distress alarm connected to the Sheriff's office.

2.2.6. Any person activating the door bell beside the main entrance should be spoken to through the intercom system. If they are an authorized user agency employee, or claim to be, the computer room operator should activate the electric strike to the outer door. The employee should then follow the procedures prescribed in 2.2.2. through 2.2.5. If other persons denied admittance refuse to leave the area, the Sheriff's Department should be notified.

2.3. Roof checks

2.3.1. If the computer room employee hears unexplainable noises on the roof or anywhere on the exterior of the building, he or she should notify the Sheriff's Department.

2.3.2. The door to the roof is alarmed. If the air conditioning system appears to be malfunctioning to the extent that the computer room employee must inspect the chilling units, he or she should call the Sheriff's Department and inform the Communications Center operator that he will open the roof door in so many minutes and that an alarm condition will show. The Communications Center operator will then call the computer room back to verify that a computer room employee made the call.[1/] The employee will then tell the communications center operator how long he expects to be on the roof and that he will call the Sheriff's Department back before the end of the time period. If he does not, the Sheriff's Department will dispatch an officer to the facility.

[1/] This arrangement must be coordinated by agreement with the Sheriff's Department.

END