COMPUTER CENTER PHYSICAL SECURITY AND DISASTER RECOVERY
PHYSICAL SECURITY EVALUATION

CONTENTS PAGE

1. GENERAL

1.01 This aid has been developed by a multicompany GUARDSMAN project team under the direction of AT&T Information Systems Technical Support and Standards. This aid is issued by the AT&T Director—Information Systems Planning and Support for implementation by Bell System Companies.

1.02 Whenever this section is reissued, the reason(s) for reissue will be given in this paragraph.

1.03 As referenced in Section 007-590-302, the purpose of this section is to provide a tool for evaluating the present physical security system in each computer facility. All questions should be answered with "Yes," except where indicated by a double asterisk (**). "No" answers indicate weaknesses or potential weaknesses in existing security systems and should be investigated. On the question marked by **, the correct answer is "No." A "Yes" answer would indicate a weakness or potential weakness in existing security systems.

2. SURVEY

EXPOSURE TO FIRE HAZARDS

A. Construction

	YES	NO
1. Is the computer housed in a building constructed of fire-resistant and noncombustible materials?	____	____
2. Is the subflooring concrete or noncombustible with positive drainage?	____	____
3. Is the raised flooring constructed of aluminum or other noncombustible material?	____	____
4. Is the underfloor cabling channeled through conduits?	____	____
5. Is the floor tile nonpetroleum based?	____	____
6. Are the walls and trim noncombustible and painted with water-based, fire-retardant paints?	____	____
7. Are doors, partitions, and framing made of noncombustible materials?	____	____
8. Is all glass of the steel-mesh or reinforced type?	____	____
9. Is the ceiling tile made of noncombustible materials (including supports)?	____	____
10. Are cables connecting ceiling lights placed in conduits?	____	____
11. Has sound-deadening materials (on walls, in cabinets, or around desks and operating positions) been sprayed with fire-retardant chemicals? (Foamed cellular plastics should never be used.)	____	____
12. Is the position of the computer facility in an area away from potential hazards such as fire, cafeterias, power cabling, rubbish storage, caustic chemicals, fumes, odors, etc?	____	____
13. Have steam lines been removed from the proximity of the computer facility?	____	____
14. Is the computer facility near areas employing hazardous processes?**	____	____
15. Have hazards been removed from the immediate surrounding area?	____	____
16. Are the computer facility and the supporting facilities separated sufficiently by fire-resistant materials to prevent fire in one area from affecting other areas:		
(a) Tape or disk libraries?	____	____
(b) Paper or card storage?	____	____
(c) Backup files?	____	____
(d) Source decks?	____	____
(e) Source listings?	____	____

	YES	NO
(f) Supporting operating facilities?		
(1) Alternate computing facilities?	____	____
(2) Punch card processing facilities?	____	____
(3) Remote job entry facilities?	____	____
(4) Customer engineer facilities?	____	____
(g) Copies of operations procedures?	____	____
(h) Copies of control procedures?	____	____
(i) Forms handling equipment?	____	____
(j) Report distribution facilities?	____	____

Note: Certain facilities may be located far apart and yet be subject to interpropagation via cable routing through vertical cable chases.

17. Are the facilities housing the activities listed in 16 above constructed of fire-resistant and noncombustible material?	____	____
18. If a fire were to occur in a computer facility, would other offices of the business be disabled as well?**	____	____
19. Are computer room walls extended above the false ceiling to the roof?	____	____
20. Is there sufficient room between units to permit free airflow and heat dissipation?	____	____
21. Does the construction of the facilities permit distribution of detection sensors and extinguishing systems?	____	____
22. Are exits and fire evacuation routes clearly marked?	____	____

B. Combustibles

	YES	NO
1. Are paper and other supplies stored outside the computer area?	____	____
2. Are curtains, carpets, furniture, and drapes fire-retardant treated or noncombustible?	____	____
3. Are caustic or flammable cleaning agents permitted in the computer facility?**	____	____
4. If flammable cleaning agents are permitted in the computer facility, are they kept in small quantities and in approved containers.	____	____
5. Is the quantity of combustible supplies stored in the computer facility kept to the minimum?	____	____
6. Is the space beneath the access flooring used for storage of class A combustible materials such as data processing (DP) cards?**	____	____
7. Is subfloor volume cleaned regularly?	____	____
8. Is all furniture of metal construction?	____	____
9. Are copies of listings and card decks kept in the computer facility?	____	____
10. Are clothing racks stored in the computer facility?	____	____
11. Are there excess tapes, disks, or cards in the computer facility?**	____	____
12. Is paper-bursting and shredding equipment kept away from the computer facility?	____	____
13. Is report distribution and forms handling equipment kept away from the computer facility to keep dust to a minimum?	____	____
14. Are computer facility safes closed when not being accessed?	____	____
15. Are loose pieces of plastic (such as tape rings, disk covers, tape covers, empty tape reels) kept out of the computer facility?	____	____
16. Does "decoration" of the computer facility with posters, company literature, graffiti, or holiday decoration meet the requirements of Section 760-610-200?	____	____

C. Storage

	YES	NO
1. Are critical files "backstopped" with current copies in fireproof safes or remote facilities?	____	____
2. Could the last several days processing be recaptured with copies of files and transactions remotely located?	____	____
3. Is the number of tapes outside the tape library kept to a minimum at all times?	____	____
4. Are data safes located in a separate fire hazard area other than the tape library?	____	____
5. Are disk pack storage cabinets fitted with casters to aid in emergency evacuation?	____	____
6. Are tape storage racks fitted with casters to aid in emergency evacuation?	____	____
7. Are there obstructions (risers, width of doorway, etc) that prohibit the evacuation of storage racks?**	____	____
8. Is there a wall in the tape library to secure tape racks and other equipment?	____	____
9. Have all source decks been copied to tape and stored in the data safe?	____	____
10. Are all of the user department's card files removed from the computer facility?	____	____
11. Is there a data safe located in a remote area away from the computer facility for backup protection?	____	____
12. Are cabinets housing card decks stored away from the computer area?	____	____
13. Have alternate storage facilities been selected?	____	____
14. In case of emergency, is transportation scheduled to move files?	____	____

D. Detection Equipment

	YES	NO
1. Do the facilities have one or more of the following:		
(a) Smoke detection equipment?*	____	____
(b) Humidity control equipment?	____	____
(c) Thermocouple detectors?	____	____
2. Are any of these detection units mounted ***inside*** the cabinets of critical system components?	____	____
3. Are smoke detectors installed:		
(a) In ceiling?	____	____
(b) Under raised floor?	____	____
(c) In air return ducts?	____	____
(d) In the compartment?	____	____
4. Are smoke detectors properly engineered to function in a computer facility?	____	____
5. Are detection systems tested on a scheduled basis?	____	____
6. Are smoke and fire detection systems connected to the plant security panel and municipal police departments?	____	____
7. Are underfloor smoke detector heads identified by hanging markers in the computer facility ceiling?	____	____

*Specifically recommended by NFPA.

E. Alarm Mechanism

	YES	NO
1. Do the facilities listed in A through D above provide alarm mechanisms, such as automatic alarming upon detection of fire (light), smoke, or inordinate heat rise?	____	____
2. Are there several manually operated alarm systems located strategically throughout the facility?	____	____
3. Does the alarm device report the location of the fire to a centralized or municipal fire or security position?	____	____
4. Does the alarming mechanism contain automatic shutdown of critical equipment? (Particularly required with sprinkler systems.)	____	____
5. Is there a smoke detector alarm horn in a central location in the computer room?	____	____
6. Does the alarm sound:		
(a) Locally?	____	____
(b) At watchman stations?	____	____
(c) At central station?	____	____
(d) At fire department or police headquarters?	____	____

F. Protection Equipment

	YES	NO
1. Do the facilities have one or more of the following:		
(a) Automatic dispersal of a fire extinguishing or retardant agent, such as:		
(1) Gas-Halon 1301 (above and beneath floors and ceilings)? Have personnel been trained both in the use of the gas and personal safety measures?	___	___
(2) Foam?*	___	___
(3) Water (last resort)?		
• Wet pipe (releases water at a set temperature)?	___	___
• Preaction (may sound an alarm and delay release of water)?	___	___
(4) Fixed flooding systems?	___	___
(b) Manual equipment, such as:		
(1) Portable extinguishers for electrical and other fires?	___	___
(2) Are portable fire extinguishers located strategically around the area with location markers clearly visible over computer equipment?	___	___
(3) Water or other extinguishing agent for nonelectrical fires?	___	___
(4) Are extinguishers located throughout the facilities where they can be easily obtained within a few steps?	___	___
2. Automatic and/or delayed interruption of power sources where electric fires have been discovered?	___	___
3. Automatic shutdown of air conditioning systems (particularly where Halon 1301 is used)?	___	___
4. Automatic shutdown of heating or humidity systems?	___	___
5. Automatic close off of air ducts?	___	___
6. Automatic illumination of emergency lighting on interruption of the prime power source?	___	___
7. Automatic sealing of firebreaks or fire doors between sections of the facility?	___	___
8. Are there any fire suppressant outlets mounted ***inside*** the cabinets of critical system components?	___	___
9. Is there a means of manually activating an automatic system?	___	___
10. Are automatic devices "rate compensated" to allow for sudden increases in temperature?	___	___

	YES	NO
11. Does emergency power shutdown include the air conditioning system?	____	____
12. If a total flooding fire protection system is installed, does it have a manual override abort capability?	____	____

*Not recommended by NFPA.

G. Reaction Planning

	YES	NO
1. Have building engineers analyzed the fire detection system to ensure that the number and location of detectors are appropriate for the ***current*** configuration?	____	____
2. Is there around-the-clock watchman coverage during nonworking hours?	____	____
3. Do procedures exist to "rearm" any fire prevention equipment?	____	____
4. Does the construction of the facilities permit easy access by fire-fighting personnel and equipment?	____	____
5. If access is through an electrically controlled system, can it be operated by standby battery power?	____	____
6. Are emergency power shutdown controls easily accessible at points of exit?	____	____
7. Can emergency crews gain access to the computer room without excess delay even during off shifts and holidays?	____	____
8. Are additional floor panel removers installed adjacent to fire extinguishers?	____	____
9. Have locations been identified and have personnel been informed of and provided instruction on the operation of the sprinkler shutoff valve for annexes, computer operations, and data entry?	____	____
10. Does the fire department know the location of both the computer room and flashing red lights or other alarm devices? Is there a reception area that contains indicators of alarm conditions in the computer facility?	____	____
11. Is there a battery-powered megaphone available, and are personnel knowledgeable of its location and operation?	____	____
12. Are fire drills held regularly?	____	____
13. Are operators trained periodically in fire-fighting techniques and assigned individual responsibilities in case of fire?	____	____
14. Is the no-smoking prohibition in the computer room and tape library strictly enforced?	____	____
15. Is there a documented Disaster and Security Plan?	____	____
16. Is there an area "Fire Warden" appointed?	____	____
17. Is the alarm tested regularly?	____	____
18. Are there "simulated" disasters to exercise an evacuation plan?	____	____
19. Is a fire inspection conducted periodically by organizational or municipal fire officers?	____	____
20. Are fire and evacuation plans easily available and reviewed periodically with the staff?	____	____

	YES	NO
21. Is the use of incendiaries controlled within the facilities?	____	____
22. Is there a regular inspection by qualified personnel of all automatic detection and protection systems?	____	____

WATER HAZARD/DAMAGE EXPOSURE

Physical Location

	YES	NO
1. Are computers excluded from areas below grade?	____	____
2. If not, have sufficient sealing and foundation draining devices been included?	____	____

A. Within the Facility

1. Are overhead steam or water pipes (except sprinklers) eliminated?	____	____
2. Is there sufficient drainage under the raised floor to remove accumulated liquid quickly?	____	____
3. Are drains installed on floor above the facility to divert accumulated water from all hardware?	____	____
4. Is the upper ceiling constructed so as to conduct water from higher levels away from the computer facility?	____	____
5. Is the floor above the facility watertight?	____	____
6. Are the pipe and wire openings watertight?	____	____
7. Is there adequate drainage to prevent water overflow from adjacent areas?	____	____
8. Is an industrial-type vacuum cleaner (one that will pick up water) readily available to computer facility?	____	____
9. Is there a dispenser for tarpaulins (tarps) to be used for covering the hardware in the event the sprinkler heads discharge?	____	____
10. Are all electrical junction boxes under the raised flooring held off the slab to prevent water damage?	____	____
11. Are there sufficient ducts to conduct water used in air conditioning systems away from the building?	____	____

B. Outside the Facility

1. Is the roof sufficiently sealed to prevent opening and subsequent leakage caused by wind damage?	____	____
2. Is there protection against accumulated air conditioning water or leaks in rooftop water towers?	____	____
3. Are exterior windows and doors watertight?	____	____
4. Is grading around the exterior of the facility constructed to conduct water away from the building?	____	____
5. Are there sufficient storm drain inlets to accommodate water accumulation during sudden or seasonal rainfall?	____	____
6. Have subterranean or underroof heating systems been installed to melt snow?	____	____

AIR CONDITIONING CONSIDERATIONS

A. Air Conditioning Facility

	YES	NO
1. Are the BTU ratings of air conditioning equipment appropriate for the facility?	___	___
2. Is the air conditioning system used exclusively for the computer area?	___	___
3. Is there a backup air conditioning capability?	___	___
4. Is the compressor remote from the computer facility?	___	___

B. Intakes, Ducting, and Piping

1. Are duct linings and filters noncombustible?	___	___
2. Are air intakes:		
(a) Covered with protective screening?	___	___
(b) Located well above street level?	___	___
(c) Located so as to prevent intake of pollutants or other debris?	___	___
3. Could ducting carry fumes and smoke to other offices?**	___	___

C. Shutdown

1. Are there alternate locations in the computer facility area where all power and air conditioning fans for the area can be shut off?	___	___
2. Can installed ceiling exhaust fan(s) provide sufficient air movement should the air conditioning system become inoperable for several hours?	___	___

D. Protection

1. Is the cooling tower fire protected?	___	___
2. Are sensors installed within the air conditioning system?	___	___
3. Does the construction of the air conditioning facilities permit only authorized access, including:		
(a) Placement in high place to restrict access?	___	___
(b) Protection of the water supply source?	___	___
(c) Protection of fan or cooling mechanisms?	___	___
(d) Survey of air conditioning area by closed circuit television?	___	___
(e) Periodic check by security personnel?	___	___

	YES	NO
4. Do security personnel have copies of wiring, ducting, water, and air flow diagrams for use by maintenance or fire-fighting personnel?	____	____
5. Is there heat or humidity control equipment?	____	____
6. Are there temperature and humidity monitoring and recording devices?	____	____

ELECTRICAL CONSIDERATIONS

A. Power Supply

	YES	NO
1. Is the local electrical power reliable?	____	____
(a) Is there sufficient amperage to support the facility when all equipment is operating?	____	____
(b) Is the power supply susceptible to:		
(1) "Blackouts"?**	____	____
(2) Reduced operating voltages?**	____	____
(3) Surges or power "spikes"?**	____	____
(c) If electrical power is unreliable, have alternate power sources been investigated?		
(1) Secondary sources?	____	____
(2) Standby generators?	____	____
(d) Is the voltage input monitored with a recording voltmeter that displays changes?	____	____
2. Does the data center have a devoted power system? (The source of power should not connect to other parts of the organization.)	____	____
3. Is there an alternate power source that permits resumption of operation if the prime power source is destroyed?	____	____
4. Is needed air conditioning connected to this alternate source?	____	____

B. Wiring

1. Is wiring in conformance with local building codes for the installation's class of service?	____	____
2. Do security and maintenance officials have a copy of the wiring diagram?	____	____
3. Are electrical boxes placed in areas not exposed to water or other potential damage?	____	____
4. Are the main power control boards in a remote or restricted access position?	____	____
5. Are there emergency power-off switches at each exit of the computer room to meet OSHA requirements?	____	____
6. Has all wiring under the raised floor in the computer facility been checked, assuring that all circuits (including 110 volt) are wired to shunt breakers and are properly grounded?	____	____
7. Are all power panels supplying the computer facility locked?	____	____
8. Are all circuit breakers/fuses clearly labeled?	____	____

C. Lighting

	YES	NO
1. If there is an emergency lighting system, has it been recently tested?	____	____
2. If the system has fixed position lamps, have they been tested to determine if they illuminate the proper area?	____	____
3. Are there sources of light, strategically located, that do not depend upon the main power source?	____	____
4. Is there an emergency power source to energize emergency lighting?	____	____
5. Are the office lights wired to provide a security night-light?	____	____
6. Have emergency lights for the computer facility, annex, and data entry area been installed?	____	____

PREPARING FOR CIVIL, MAN-MADE, AND NATURAL DISASTERS

A. Location

	YES	NO
1. Is the facility remote from any earthquake fault?	____	____
2. Is the facility located in a riverbed or floodplain?**	____	____
3. Is the facility close to high voltage transmission lines?**	____	____
4. Is the facility close to heavily traveled highways?**	____	____
5. Is the facility close to rail lines?**	____	____
6. Is the facility close to fuel storage containers?**	____	____
7. Is the facility close to fuel or steam transmission lines?**	____	____
8. Is the facility close to an isolated metal structure that might draw lightning?**	____	____
9. Is the facility located in a high crime area?**	____	____
10. Have there been reports of local civil unrest vis-a-vis computer facilities?**	____	____
11. Is the facility in an area of high fire potential?**	____	____
12. Is the facility close to an airport?**	____	____
13. Is the facility close to the storage or processing of toxic or caustic chemicals?**	____	____
14. Is the facility located in an area of dense trees or other tall foliage?**	____	____
15. Is the facility located in an area where flora is allowed to dry, ripen, or compost?**	____	____
16. Would disasters occurring in adjacent structures have a deleterious effect on your facility?**	____	____
17. Is the facility located where problems with small animals and/or rodents might occur?**	____	____

B. Construction

1. Is the building structurally sound:		
(a) To resist windstorms and hurricanes?	____	____
(b) To resist flood damages?	____	____
(c) To resist earthquakes?	____	____
2. Are building and equipment properly grounded for lightning protection?	____	____
3. Is the building on a solid foundation?	____	____

	YES	NO
4. Is the building constructed so as to be "defensible" in the case of civil unrest?	____	____

C. Natural Disaster Prediction

1. Are there some means to advise personnel of possible natural disaster?	____	____
2. Is there a series of contingency steps that are invoked when a natural disaster advisory is received?	____	____

D. Man-Made Disaster Prediction

1. Will appropriate personnel be notified in the case of a nearby disaster, such as fire in adjacent buildings?	____	____
2. If the facility is in the flight path of an airport, will appropriate personnel be notified of potential aircraft difficulty?	____	____

ACCESS CONTROL CONSIDERATIONS

A. Identification

	YES	NO
1. Is advertising the location of this computer facility discouraged?	____	____
2. Is access to the computer area restricted to selected personnel?	____	____
3. Is there a photo-badge system for positive identification of employees?	____	____
4. Do mechanisms exist to ensure that the person is carrying his/her own badge?	____	____
5. Does the computer facility have a current photograph of every person with legitimate access to the area?	____	____
6. Is a person admitted merely because he/she is known?**	____	____
7. Is a person admitted merely because he/she is accompanied by a known person?**	____	____
8. In the case of temporary badges, is the badge matched against some other form of identification?	____	____
9. Are identification badges color-coded, facility-zoned, or marked to indicate security clearance or access?	____	____
10. Are transient personnel checked ***out*** of as well as into the computer facility?	____	____
11. Can anyone ask for and receive data files or reports?	____	____
12. If not, is there a procedure to ensure:		
(a) Security clearance of the individual relative to the files or reports sought?	____	____
(b) The "need to know" access permitted relative to the files or reports sought?	____	____
13. Are ***all*** visitors challenged?	____	____
14. Are people free to carry ***anything*** in and out of the facility?**	____	____
15. Are food and beverages prohibited in the computer room?**	____	____

B. Access Routes

1. Are there guards on all street entrances that lead to the computer area?	____	____
2. Do hallways have false floors that could permit unauthorized access to the computer facility?**	____	____
3. Are accesses from stairways restricted or in any way controlled?	____	____
4. Are access routes to and from nearby offices controlled?	____	____
5. Are all exterior windows at or near street level covered with expanded metal grills?	____	____

	YES	NO
6. In areas with a high crime rate, is there bulletproof glass?	___	___
7. Is there a "dumbwaiter" or freight elevator that could be used as an unauthorized access route?**	___	___
8. Is access controlled from a loading dock?	___	___
9. If the facilities have electrically operated doors, can they be opened manually if the power source is interrupted to gain unauthorized access?**	___	___
10. Is the computer facility screened so that it is not visible from the street?	___	___
11. If not, could access be gained through street level windows?**	___	___
12. Are the doors to the computer facility and annex locked during second shift, third shift, and weekends?	___	___

C. Visitor Control

1. Is there a visitor control procedure?	___	___
2. Is there a computer room sign in/out log for visitors?	___	___
3. Are "temporary passes" numbered to permit control of the pass as well as the person using it?	___	___
4. Is there a procedure for returning and accounting for temporary passes?	___	___
5. Can temporary passes be duplicated easily?**	___	___
6. Are pass and access rules consistently enforced?	___	___
7. Can anyone who wants to see the data center do so upon request?**	___	___
8. Are vendor personnel allowed to "roam freely" because of their apparent vendor affiliation?**	___	___
9. Is the casual visitor eliminated by stopping organization executives from including the data center in a facilities tour?	___	___
10. Does someone accompany ***all*** visitors?	___	___
11. Are visitors excluded from sensitive areas of the facility?	___	___
12. Are visitors controlled under the suggestions for access contained in these guidelines?	___	___
13. Where sensitive data or files are concerned, is there ***positive*** security clearance for the visitor?	___	___

D. Security

	YES	NO
1. Is it possible for someone to access communications lines externally?**	____	____
2. Have identification markings been removed from power rooms, communications closets, etc?	____	____
3. Once open, do cabinet doors permit room for a person to work on the device?	____	____
4. Are there magnetic sensors in access doorways?	____	____
5. Are there security guards at data center accesses?	____	____
6. Are critical files "under lock and key," limiting the access?	____	____
7. Is there a periodic security check of all personnel?		
(a) Spot inspection under operation?	____	____
(b) Complete background investigation on hiring?	____	____
(c) Thorough investigation of all personnel with access to the data center?	____	____
8. Can all external doors be locked on command?	____	____
9. If there is a closed circuit television, is it monitored at all times?	____	____
10. Are there double-door arrangements that will "lock in" an intruder between them?	____	____
11. Are the security precautions the same at every entrance, including the loading dock?	____	____
12. Are plans and blueprints for the data center and other important areas controlled or restricted?	____	____
13. Is access to communication equipment, such as junction boxes, switching mechanisms, terminal outlets, etc, freely available?**	____	____
14. Are there restrictions on the introduction of camera or other photographic recording equipment in the data center?	____	____
15. Are there restrictions on the introduction of sound magnetic recording equipment, radios, or other electronic devices in the computer facility area?	____	____
16. Is metal detection equipment available? Is it used?	____	____
17. Is there a means to inspect parcels and other articles moved in and out of the data center?	____	____
18. Are there "alert" mechanisms for the summoning of security personnel?	____	____
19. Are there electric eye or proximity warning indicators positioned in infrequently used rooms or hallways?	____	____
20. Have self-closing mechanisms been installed on all internal doors?	____	____

		YES	NO
21.	Are internal doors and passageways free of all obstructions, including wedges?	____	____
22.	Are internal aisles wide, straight, and free of obstructions?	____	____
23.	Is all equipment positioned so that access doors open fully and freely?	____	____
24.	Are there external walls and windows that permit easy access to a saboteur?**	____	____
25.	Are monitoring devices connected to access doors, emergency exits, and windows for the computer room and annex, connected to the company security system?	____	____
26.	Are master key locks removed from the exterior of emergency exits?	____	____
27.	Are file areas segregated so that only specific individuals have access to them?	____	____
28.	Are PLEXIGLAS* windows installed between the data entry area and the computer room and between the computer room annex and computer room to reduce the personnel traffic?	____	____
29.	Are master controls for detection and suppression systems located outside the data center?	____	____
30.	Are communication devices and equipment relative to the computer facility in a remote or restricted access area?	____	____
31.	Is the computer room located in an inner core of the building and off the street floor and/or out of the basement?	____	____
32.	If not, are the glass windows impact resistant and protected by steel bars, grills, or mesh screens?	____	____
33.	Does the computer center have an automated access control system which provides a documented log (including employee identification, date, time, and location) of all authorized employees' entries and exits on a 24-hour basis?	____	____
34.	Is this access control system designed to restrict entry to this particular building and/or to a particular room within this building on certain days and at designated times?	____	____
35.	Does this access control system include a security buffer zone or mantrap which is located at the entrance of the computer center or computer room? (Small vestibule area with an interlock exterior door and interior door through which a person must pass to display proper identification and be relieved of any magnetic or radio frequency device before entering the computer center or computer room.)	____	____
36.	Does the access control system automatically log, and/or signal by, alarm attempts of unauthorized entry (ie, use of invalid identification or entry card, unauthorized employee or nonemployee following an authorized employee through a restricted door, compromised intrusion alarm, etc)?	____	____
37.	Are separate entrances used by personnel and delivery of supplies, packages, mail, etc?	____	____

*Trademark of Rohm & Hass Co.

	YES	NO
38. Is a separate, specially constructed room utilized for receiving, inspecting, and opening of supplies, packages, mail, etc? Are incoming packages X-rayed?	____	____
39. Is there a material pass system for inspecting incoming and outgoing items, packages, etc?	____	____
40. Is the library or storage room for magnetic tapes and disks located adjacent to the computer equipment space?	____	____
41. If so, is the room adequately secured and is the entrance door equipped with the appropriate lock or other protective device, ie, card reader?	____	____
42. Are periodic inventories of the tapes and disks made by an assigned employee; are the results of the inventories documented and retained?	____	____
43. Are tapes regenerated periodically? (It is recommended that tapes be rewound annually and that 5 percent of the tapes be test read.)	____	____
44. Is a computer maintenance room located near the equipment area to provide on-site maintenance on the equipment?	____	____
45. Are locked cabinets and/or vaults used to store sensitive data files, backup files, associated operating procedures, and documentation?	____	____
46. Are company contractors, vendors, and/or consultants required to sign nondisclosure agreements which have been approved by the appropriate departments, including Legal?	____	____
47. Are the local police and fire department basically familiar with the construction and equipment within the center to take the appropriate action in cases of emergency?	____	____
48. Are all outside utility service entrances (ie, gas, electric, water, telephone circuits, etc), including control valves, meters, and terminals, constructed and located in a manner to prevent tampering or destruction?	____	____
49. Is the control principle of division of responsibilities and rotation of assigned personnel in various duties effectively used by computer center management personnel?	____	____
50. Has a background check been conducted on all personnel assigned to the computer center?	____	____
51. Are all personnel assigned to the computer center required to wear some prominent identification such as badges or special cards?	____	____
52. Have procedures, precautions, and/or techniques been established and implemented to prevent unauthorized access and to provide access control to the computer system and/or remote terminals? Are key locks utilized on data terminal keyboards? Are keys controlled?	____	____
53. Is someone at the computer center presently assigned the responsibilities of administering the security measures and procedures?	____	____

	YES	NO
54. Has an emergency shutdown, evacuation, and restoration plan been formulated for each work shift?	___	___
55. Is there ever any occasion when only one person is in the computer room?**	___	___
56. Is all proprietary information material properly destroyed and/or erased prior to collection by public waste or trash collectors?	___	___
57. Are employees who handle extremely sensitive information and/or material on a daily basis required to sign a nondisclosure agreement which has been approved by the appropriate departments, including Legal?	___	___
58. Are tapes transmitted via a secure packaging? If so, are company mail or vehicles used?	___	___

Chain Link Fence: If the perimeter of the computer facility is protected by a chain link fence, the following items should be considered.

59. Is the fence constructed of adequate gauge wire, generally No. 11 gauge or heavier?	___	___
60. Is the mesh opening in the fence no larger than a 2-inch square?	___	___
61. Is the bottom of the fence embedded in a suitable material to a minimum depth of 3 inches or secured to barbed wire at or below ground level?	___	___
62. Are the fence posts 6 feet on center and embedded in cement?	___	___
63. Are sufficient steel tie wires used to secure the fence to the posts?	___	___
64. Is the distance from the ground to the top of the fence at least 7 feet (height sometimes dependent on zoning and/or city, county, etc, ordinance)?	___	___
65. If the fence joins other structures (fences or buildings), generally not recommended, is adequate protection available to prevent unauthorized entry or exit?	___	___
66. Do the fence and gates have three strands of barbed wire offset from the vertical to both the interior and exterior of the property and upward at a 45-degree angle?	___	___
67. Are the 4-point barbs, generally No. 12 gauge wire or heavier, spaced 4 inches apart?	___	___
68. Do the fence or gates need repair at any location?	___	___
69. Is the fence equipped with an alarm?	___	___
70. Is the alarm operative?	___	___

Other Type Barriers: If the perimeter of the computer facility ***is not*** protected by a chain link fence, consideration should be given to the following items.

71. Is the facility defined by any type barrier (ie, masonry wall, shrubbery, etc)?	___	___
72. If so, is the barrier adequate?	___	___

	YES	NO
73. If no barrier is present, is one warranted?	___	___
74. If so, will the recommended barrier be acceptable by the zoning and/or city, county, etc, ordinance?	___	___

Barrier Hazards: Regardless of the type of perimeter barrier present, consideration should be given to the following.

75. If there are openings in the barrier (ie, culverts, tunnels, manholes for sewers and utilities, etc), are they properly secured?	___	___
76. Is the area surrounding the barrier clear of any growth of objects (ie, trees, overhanging limbs, poles, motor vehicles, stored materials, etc) that could provide cover or assistance to persons seeking unauthorized entry?	___	___
77. Is the distance between the enclosed building and the perimeter barrier sufficient to prevent unauthorized entry or exit or possible detection of such?	___	___
78. Is protection provided (ie, guard rails, etc) inside the perimeter barrier to protect same from damage by company vehicles and to prevent vehicles from parking adjacent to the barrier in order to deter unauthorized entry or exit to the facility?	___	___
79. Is the employee parking area separated from the company parking area by a fence or wall?	___	___
80. If employee parking is permitted inside the perimeter barrier with company vehicles, are security precautions taken when employees visit their personal vehicles?	___	___
81. If company parking is provided for employees, are employee identification cards and/or vehicle decals utilized to prevent unauthorized parking, access, etc?	___	___

Entrance and Exit Gates: Consideration should be given to the following items in connection with the perimeter barrier entrance and exit gate to the computer facility.

82. If double gates are used, are they constructed in a manner to prevent them from being forced open?	___	___
83. Are there any openings around the gates larger than 6 inches?	___	___
84. Are gate hinge pins installed in such a manner to prevent the gate from being removed by lifting, etc?	___	___
85. If a chain is used for locking the gate, is it welded to the gate or adjoining post to prevent its removal?	___	___
86. Is the padlock (combination lock not recommended) welded to the chain to prevent its removal?	___	___
87. Are padlocks changed periodically depending upon employee turnover, lost keys, major thefts, etc?	___	___
88. Is someone assigned the responsibility of key control and inventory?	___	___

	YES	NO
89. If automatic or electrical gate is installed, are the controls located and operated from inside the gates to prevent unauthorized entry?	____	____
90. Are the serial numbers removed from the locks to prevent someone from obtaining duplicate keys?	____	____
91. Are all gates locked when the facility is unattended?	____	____
92. Is someone at the facility assigned the responsibility of securing the entrances or exits after all persons have departed?	____	____
93. Are gates, which are not in use, inspected frequently to make sure they remain locked and in good condition?	____	____
94. If the gate is equipped with an alarm, is it operative?	____	____
95. If closed circuit television is utilized to observe the gate, is it operative?	____	____
96. Is responsibility for the monitoring assigned?	____	____
97. If contract guard service is utilized, is the guard(s) present and alert?	____	____
98. Are informational, warning, or no trespassing signs bilingual (two appropriate languages), when necessary, and legally posted?	____	____

Outside Lighting: Consideration should be given to the following items in connection with the perimeter lighting.

99. Is the perimeter lighting sufficient to provide detection of authorized entry? Are these lights reduced due to an energy conservation program?**	____	____
100. Is the lighting sufficient at the entrance gate for identification of individuals and verification of credentials?	____	____
101. Is the lighting at each building entrance sufficient for security purposes?	____	____
102. If closed circuit television is utilized, is lighting sufficient for its use?	____	____
103. Were all lights operative at the time of inspection?	____	____
104. Do light beams overlap to provide coverage in case a bulb burns out?	____	____
105. Is there a dependable auxiliary source of power for the lighting system?	____	____
106. Are all lighting fixtures and wiring installed beyond easy reach?	____	____
107. Are protective lighting guards provided at necessary locations within the perimeter to prevent intentional breaking of bulbs?	____	____
108. If contract guards are provided, is there sufficient light for them to detect movement at all points within the perimeter barrier?	____	____

	YES	NO
109. Is the lighting system controlled by photoelectric cells or locked time clocks which are more reliable than manual operation?	____	____
110. Is someone assigned the responsibility of inspecting and maintaining the lights on a scheduled basis?	____	____
111. Are outside lights utilized for deterring unauthorized entry?	____	____

HOUSEKEEPING

	YES	NO
1. Is there an accumulation of trash in the computer area?**	____	____
2. Are equipment covers and work surfaces cleaned regularly?	____	____
3. Are floors washed regularly?	____	____
4. Are wastebaskets emptied outside the computer area to reduce dust discharge?	____	____
5. Is carpeting of the antistatic type?	____	____
6. Are low fire hazard waste containers used?	____	____
7. Are maintenance areas kept clean and orderly?	____	____
8. Is there a mandated and enforced housekeeping procedure that ensures that flammable materials (such as paper, inks, corrugated boxes, and ribbons) are kept to a minimum?	____	____
9. Are closed circuit TV lenses cleaned regularly?	____	____

OTHER FACILITY CONSIDERATIONS

	YES	NO
1. Are security and operations personnel briefed on how to react to civil disturbances?	____	____
2. Is there a good liaison program with local law enforcement agencies?	____	____
3. Do personnel know how to handle telephone bomb threats?	____	____
4. Are dry-cell lanterns available for computer room emergency use?	____	____
5. Are door hinges on all doors to the computer room and computer room annex welded?	____	____
6. Is there a paper shredder to destroy confidential reports?	____	____
7. Are there metal trash receptacles with hinged covers?	____	____
8. Have locks been installed on the windows connecting the data entry area and computer operations?	____	____
9. Is the data center in proximity to the organization's medical facilities?	____	____

PERSONNEL

	YES	NO
1. Are supervisors alert to the possible disgruntled employee?		
(a) Conflict between employees?	____	____
(b) Dissatisfaction over pay, company policies, or other company-related incidents, such as working conditions, work period, or performance evaluation?	____	____
(c) Possible personal problems with family, finances, etc?	____	____
2. Do personnel policies allow for containment or immediate dismissal of employees who may constitute a threat to the installation?		
(a) Notification procedures?	____	____
(b) Minority considerations?	____	____
(c) Political considerations?	____	____
3. Do supervisors know their people well enough to detect a change in their living habits?		
(a) Financial status?	____	____
(b) Living conditions?	____	____
(c) Clothing, automobile, etc?	____	____

TRAINING ORIENTATION

	YES	NO
1. Is there a continuing personnel education program in computer security?	____	____
2. Are the personnel trained for an orderly shutdown of the equipment for various types of emergencies, such as fire, earthquake, and bomb threat?	____	____
3. Are there orientation sessions dealing with emergency procedures?	____	____
4. Has a fire extinguisher demonstration been held for all operators?	____	____
5. Have computer operators attended a class of computer room security?	____	____
6. Are people cross-trained to cover all functions?		
(a) Can more than one operator on each shift operate each piece of hardware?	____	____
(b) Can more than one operator on each shift run each system?	____	____
(c) Can more than one person on each shift perform each emergency task?	____	____
(d) Does each person have a primary and secondary emergency assignment?	____	____
7. Are key personnel, at the minimum, trained in first aid procedures to treat burns and smoke inhalation (such as hydrogen chloride gas from insulation)?	____	____
8. Is first aid equipment available within the facilities and do key personnel know its location and contents?	____	____
9. Have all personnel been trained in the use of fire-fighting equipment.	____	____

OPERATING PROCEDURES

	YES	NO
1. Are meter hours correlated with utilization hours?	____	____
2. Has an acceptable range of correlation of meter versus utilization hours been established?	____	____
3. Do employees have access to tools with which they might do harm or "experiment" with the hardware?**	____	____
4. Are scheduled maintenance activities monitored to assure proper reliability and hardware performance?	____	____
5. Is there a mechanism to verify that maintenance ***claimed*** is maintenance ***performed?***	____	____
6. Have record systems indicating vendor, model numbers and features, and level of engineering change been established?	____	____
7. Are all periods of downtime verified?	____	____
8. Does each period of downtime have a corresponding maintenance request?	____	____
9. Are "end meter" with "begin meter" readings checked each morning for unexplained gaps?	____	____
10. Are steps taken to resolve unexplained time periods?	____	____
11. Is all incoming work checked against an authorized user list?	____	____
12. Is output spot-checked for possible misuse of the system?	____	____

TAPES AND/OR DISKS

	YES	NO
1. Is there a procedure for tape and/or disk accountability?	____	____
2. Does the tape and disk accountability procedure cover:		
(a) Frequency of use?	____	____
(b) Frequency of cleaning?	____	____
(c) Authorized user?	____	____
(d) Security classification?	____	____
(e) External evacuation classification?	____	____
(f) Release procedures?	____	____
3. Are magnetic tapes and disks filed in an orderly manner?	____	____
4. Is there a tape and/or disk cleaning plan?		
(a) Are tapes cleaned on a regular basis?	____	____
(b) Are disk packs checked and cleaned?	____	____
5. Are tapes kept in their containers except when in use?	____	____
6. Are tapes stored vertically?	____	____
7. Are tape utilization records maintained?	____	____
8. Are tape containers cleaned periodically?	____	____
9. Are tape heads cleaned every shift?	____	____
10. Are tapes sample-tested periodically for dropouts to determine the general condition of the tape library?	____	____
11. Is frayed leader stripped regularly?	____	____
12. Has the possibility of a tape rehabilitation or recertification program been investigated?	____	____
13. Is the tape library located in an area not subject to explosion or other dangers?	____	____
14. Are storage vaults specifically designed for magnetic media used for critical tape files?	____	____
15. Has magnetic detection equipment been considered to preclude the presence of a magnet near tapes and disks?	____	____
16. Is similar protection provided for tape files while in transit to a backup site, etc?	____	____

FILE, DOCUMENTATION, AND DATA

	YES	NO
1. Are duplicate files stored in a building separate from that containing the originals?	____	____
2. Is there a current inventory of such files?	____	____
3. Have the merits of leasing underground storage space from a reputable vital records concern been considered?	____	____
4. Are programs stored in a low fire-hazard container?	____	____
5. Has a "dry run" been held in the past 3 months to test the ease and accuracy of the file backup system?	____	____
6. Are program changes controlled and recorded?	____	____
7. Are changes made only to a copy of a program file, but not to the original?**	____	____
8. Is a record maintained of items withdrawn from the production file area?	____	____
9. Does the computer operations department review systems documentation for compliance with operational standards?	____	____
10. Is there a backup of source data for programs under development?	____	____
11. Are all computer room and data entry tape files retained for at least 5 days?	____	____
12. Are all payroll JCL controlled and accessed only by a minimum of operators?	____	____
13. Have data, programs, and documentation been classified in terms of criticality to the organization?	____	____
14. Is there a marking system for evacuating the most critical items first?	____	____
15. Are data files of the highest classification together in racks to permit easy removal?	____	____
16. Is system backup (disk-to-tape-to-disk) done weekly? Is JCL backup (card-to-tape) done bimonthly?	____	____
17. Is there restricted access to all JCL for confidential jobs?	____	____

**INDICATES "No" answer. "Yes" answers in these areas are potential security weaknesses and require future investigation.