COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

Note: The following controls are summaries of the guidelines in SW 007-590-905, except those with the description "Optional." Optional controls are not required by practice, but if adhered to, can enhance a facility's physical security.

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
FIRE CONTROLS		
3.02	Computer rooms are not located directly above, below, or adjacent to:	
	a. Parking garages	
	b. Loading docks	
	c. Cafeterias/snack bars	
	d. Building power rooms	
	If no, adequate protection features have been provided	
3.03	Computer facility computers or peripheral equipment maintained on floors above the sixth floor	
	If yes, fire fighters can manage equipment at floors 7 and above	
3.04	Walls encompassing computer rooms	
	a. Slab-to-slab	
	b. One hour fire-rated noncombustible construction	
3.04	Walls encompassing magnetic media operations rooms are one hour fire-rated noncombustible	
3.04	Walls encompassing magnetic media operations libraries are one hour fire-rated noncombustible	
3.05	Computer room doors at least 3/4 hr fire-rated, U.L.-listed Class C	
3.05	Magnetic media operations room doors are at least 3/4 hour fire-rated, U.L.-listed Class C	
3.05	Magnetic media operations library doors are at least 3/4 hour fire-rated, U.L.-listed Class C	
3.06	Magnetic media libraries w/o gaseous flooding system or sprinklers	
	a. Walls are two hour fire-rated	
	b. Doors are 1 1/2 hour fire-rated, U.L.-listed Class B	
3.07	Magnetic media libraries with gaseous flooding system or sprinklers	
	a. Walls are one hour fire-rated	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	b. Doors are 3/4 hour fire-rated, U.L.-listed Class C	
3.08	Computer room perimeter walls are free of windows	
	a. If no, windows have: LEXAN	
	b. ... Wired glass	
	c. ... Two panes of glass	
	d. ... High-impact glass	
3.09	Computer room doors within perimeter walls are free of glass	
	If no, glass is supported by wire	
3.14	Occupied/unoccupied cable holes/slots in slabs/walls are fire-stopped	
3.14	Shaft enclosures among floors are sealed	
3.15	Fire dampers have fire-rated listing	
3.16 4.29	Storage rooms and C.E. rooms do not open into magnetic media facilities	
3.17	Storage room doors opening into computer rooms are closed when storage rooms are unoccupied	
3.19	High fire load areas (e.g., Print-Punch, Bill Mailing and Distribution, Bursting) are not within, or do not open into, computer rooms	
3.20	Computer equipment staging areas	
	a. Located outside computer rooms	
	b. Fire, access, and environmental controls in place	
3.20	Boxes removed from computer equipment (when in computer room) are immediately removed from computer room	
3.23	Computer room walls are painted with fire-resistant paints	
3.24	Noncombustible items in computer room:	
	a. Partitions	
	b. Cubicles	
	c. Carpet	
	d. Ceiling materials	
	e. Above-ceiling insulation	
	f. Raised floor covering	
	g. Air duct insulation	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	Underfloor cable is in conduit (optional)	
3.26	Computer room trash receptacles are fire-rated	
3.27	Cleaning agents are maintained in approved containers	
3.27	Cleaning agent containers are placed in enclosed cabinets	
3.27	Computer rooms are free of combustible decorations	
3.27	Computer rooms and magnetic media facilities free of large amounts of combustible items: paper, trash, cleaning materials, etc.	
3.28	Computer rooms are free of kitchen appliances	
3.29	Floor panel lifters are available when needed	
3.30	Computer cable (when purchased) has fire-retardant properties	
3.31	Fire-detection-alarm system connected to:	
	a. Central building monitoring station (e.g., guard station)	
	b. Fire department station	
	If no, fire department notification procedures in place	
	c. Emergency power system	
3.31	Fire-detection-alarm system inspected on a scheduled basis	
3.31	Detectors detect:	
	a. Smoke	
	b. Heat	
3.31	Detectors installed:	
	a. Above dropped ceiling	
	b. Within compartment	
	c. Beneath raised floor	
	d. Outside computer facility (if computers also exist in this area)	
	e. In storage rooms next to or within computer facility	
	f. In air handling systems serving computer facility	
3.31	Fire alarms in computer room(s) are:	
	a. Audible	
	b. Visual	
3.31	Fire alarms heard throughout computer facility rooms	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
3.31	Personnel in room within computer room hear fire alarm or PA system when room's door(s) are closed	
3.31	Fire alarm activated outside computer room(s) activates alarms throughout computer room(s)	
3.31	Fire alarm activated inside computer room(s) activates alarms throughout computer room(s)	
3.36	Remote fire annunciator panel on each computer facility floor	
3.38	Fire extinguishers	
	a. Halon 1211 extinguishers used throughout computer room(s)	
	b. CO2 extinguishers used:	
	(1) Throughout computer rooms	
	(2) To supplement Halon extinguishers	
	c. Halon 1211 or water extinguishers used in paper storage areas	
	d. Fire extinguishers mounted:	
	(1) Along hallways	
	(2) In computer facility offices	
	e. Inspected on scheduled basis	
	f. Extinguishing agent immediately replenished after use	
	g. Key computer facility personnel trained in fire extinguisher use	
3.42 3.44 3.45	Total flooding systems	
	a. Water sprinklers (used in computer rooms) (optional)	
	(1) Inspected on a scheduled basis	
	(2) Can be aborted by quickly shutting off water	
	(3) Time delay (e.g., melt down of solder link)	
	b. Water sprinklers (used in magnetic media facilities) (optional)	
	(1) Inspected on a scheduled basis	
	(2) Can be aborted by quickly shutting off water	
	(3) Time delay (e.g., melt down of solder link)	
	c. Gaseous flooding systems (used in computer rooms) (optional)	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	(1) Inspected on a scheduled basis	
	(2) Can be aborted manually	
	(3) Time delay (e.g., cross-zoned detector tie-in)	
	d. Gaseous flooding systems (used in magnetic media facilities)	
	(1) Inspected on a scheduled basis	
	(2) Can be aborted manually	
	(3) Time delay (e.g., cross-zoned detector tie-in)	
3.47	Standpipe and hose system	
	a. On each floor where computer facility resides	
	b. In each computer room (optional)	
3.49	Exit signs are on computer room doors used for perimeter exit	
3.50	Exit signs are illuminated	
3.52	Emergency-exit-only doors	
	a. Open outward	
	b. Activate alarm upon opening	
	c. Sign denotes emergency-exit-only	
	d. Sign denotes alarm activation	
3.53	Fire warden for:	
	a. Building	
	b. Computer facility	
	c. Floor	
	d. Work shift	
3.53	Deputy fire warden for:	
	a. Building	
	b. Computer facility	
	c. Floor	
	d. Work shift	
3.55	Searchers for:	
	a. Building	
	b. Computer facility	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	c. Floor	
	d. Work shift	
3.57 4.58	Computer facility personnel/management are knowledgeable of building evacuation and emergency procedures	
3.58	Fire evacuation drills held annually for:	
	a. Building	
	b. Computer facility	
	c. Floor	
	d. Work shift	
3.60	Building evacuation plan in place for disabled personnel	
3.61	Emergency call list posted in each computer room	
3.62	Smoking, eating, and drinking prohibited in computer room(s)	
3.64	Annual fire inspection conducted by:	
	a. Building operations	
	b. Local fire department	
(Remaining fire controls: for data center use only; non-data-center: skip to Physical Access Controls.)		
	Bill Mailing and Distribution	
	a. Fire-detection-alarm system	
	b. Manual pull fire alarms	
	c. Fire extinguishers	
	d. Sprinkler system	
	Bursting	
	a. Fire-detection-alarm system	
	b. Manual pull fire alarms	
	c. Fire extinguishers	
	d. Sprinkler system	
	Print-Punch	
	a. Fire-detection-alarm system	
	b. Manual pull fire alarms	
	c. Fire extinguishers	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	d. Sprinkler system	
3.68	Multilevel computer room	
	a. Elevator doors are U.L.-listed Class C, 3/4 hour fire-rated	
	b. Doors to stairs meet local building code fire rating	
	c. Propped-open doors to stairs have smoke-detector-activated, magnetic door holder	
	d. Doors (in a-c) do not open into magnetic media facility	
3.69	Automatic Cartridge System (ACS) Silo(s) with Gaseous Flooding System	
	a. When Halon 1301 is discharged in silo, its:	
	(1) Initial discharge provides minimum 5% concentration for 10 seconds	
	(2) Second discharge maintains minimum 5% concentration for 10 minutes	
	b. When other agents are discharged in silo, their minimum concentration percentages and protection time frames meet NFPA 2001 guidelines	
	c. System control panels are located in computer room	
	d. System control panels have reset button	
	e. System's storage tanks:	
	(1) Located remotely from silo(s)	
	(2) Located in access-controlled room within a computer room	
	(3) If located in room outside computer room, is locked when unattended and has same fire protection as computer room	
	(4) Tested by authorized agent every six months	
	(5) Each test report maintained by system owner for six years	
	f. Power is shut off to affected silo(s) when system discharges gaseous agent	
	g. EPO procedure in place to shut off silo power during emergency outside silo	
	h. System backed up by batteries or emergency power	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	i. System has audible and visual alarms in computer room	
	j. System alarms continuously monitored at remote station	
	k. If system uses building alarm system, then system has visual alarm in computer room	
	l. System has abort capability	
	m. System abort buttons/switches located in computer room	
	n. System has discharge timer restart or manual discharge activation capability	
	o. System's fire/smoke detector-alarm has time delay feature	
	p. System time delay feature is no longer than 90 seconds	
	q. When system is in alarm:	
	(1) Persons in silos know to leave silos immediately and close silo doors as they leave	
	(2) Doors to unattended silos are closed	
	(3) No one enters a silo	
	(4) Silo and system vendors are promptly notified	
	r. Once a system discharge is completed:	
	(1) Halon 1211 (or comparable) fire extinguishers are readily available	
	(2) Affected silo(s) are fully ventilated	
	(3) Silo power restored only after silo vendor and system vendor have performed evaluation	
	s. During nonemergency periods, doors to unattended silos are in closed position	
	t. Periodic system maintenance by system vendor	
PHYSICAL ACCESS CONTROLS		
4.02	Computer rooms are all located on floors above ground level	
	If no, computer room(s) on ground floor do not have building perimeter windows	
4.04 4.05	Computer facility has physical access control system	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	If yes, then when building or computer facility security stations are not operating, physical access control system records granted and denied attempts at entry to and exit from facility by:	
	a. Name/I.D. designation	
	b. Door/room location	
	c. Time-date	
4.06	Building (housing computer facility) has building security station(s)	
	If yes, then when the station(s) operate:	
	a. Employee's company I.D. checked at station during regular work shift	
	b. Employee's company I.D. checked at station during off-hours, and manual/electronic sign-in and sign-out required	
	c. Employee without company I.D.:	
	(1) Records manual/electronic entry at station	
	(2) Assigned daily pass	
	(3) Escorted to and from computer facility by authorized manager	
	(4) Records manual/electronic exit at station	
	or	
	(1) Shows some form of I.D. to prove identity	
	(2) Records manual/electronic entry at station	
	(3) Assigned daily pass	
	(4) Returns pass to station after tour of duty and records manual/electronic exit	
	d. Controls a-c apply to vendors with vendor IDs	
	e. Vendor who is assigned interim I.D.:	
	(1) Desires access to computer facility during regular work shift:	
	(a) Assigned I.D. at security station and records entry on first day	
	(b) Shows I.D. at security station each day after that	
	(c) Escorted to facility, chaperoned when in facility, then escorted from facility by authorized manager	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	(d) Returns I.D. and records exit at station on last day	
	(2) Desires access to computer facility during off-hours:	
	(a) Adheres to items a-d in (1) above	
	(b) Records entry and exit at station each day	
	(3) Assigned physical access control device (e.g., card key) only upon entity management level approval	
	f. Visitor who is assigned daily pass:	
	(1) Records entry at station	
	(2) Assigned daily pass	
	(3) Escorted to facility, chaperoned when in facility, then escorted from facility by authorized manager	
	(4) Returns pass and records exit at station	
	g. Deliveries to, or into, a computer facility:	
	(1) Computer facility employee receiving delivery collects delivered item(s) at station (loading dock)	
	(2) Delivery person allowed to accompany delivery to computer facility. If yes, delivery person:	
	(a) Records entry in building register	
	(b) Assigned daily pass	
	(c) Escorted by computer facility manager (or manager's designee) to computer facility	
	(d) Monitored when in computer facility by computer facility manager/designee	
	(e) Upon completion of delivery, returned to station (by manager/designee), returns pass, and records exit in register	
	(3)(Optional) In-house personnel collect delivered item(s) at station (loading dock) and deliver to computer facility	
	(a) In-house personnel deliver item(s) into a computer room when computer facility manager (or manager's designee) is present	
	(b) In-house personnel monitored when making delivery in computer room	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
4.06	Familiar with Temporary Vendor/Deliverer Exception Policy (if no, see SW 007-590-905, Item 4.6.h)	
4.07	Computer facility has its own employee/guard-monitored security station(s) (optional)	
	If yes, then when the station(s) operate:	
	a. Employee's company I.D. checked at station during regular work shift against an authorized list	
	b. Employee's company I.D. checked at station during off-hours against an authorized list, and manual or mechanized sign-in and sign-out required	
	c. Employee without company I.D.:	
	(1) Presents driver's license for I.D. verification	
	(2) Records entry at station	
	(3) Assigned daily pass	
	(4) After tour of duty, returns pass and records exit	
	d. Controls a-c apply to vendors with vendor IDs	
	e. Vendor who is assigned interim I.D.:	
	(1) Desires access to computer facility during regular work shift:	
	(a) Assigned I.D. at security station and records entry at station on first day	
	(b) Shows I.D. at security station each day after that	
	(c) Chaperoned in computer facility by authorized manager	
	(d) Returns I.D. and records exit at station on last day	
	(2) Desires access to computer facility during off-hours:	
	(a) Adheres to items a-d in (1) above	
	(b) Records entry and exit at station each day	
	f. Visitor who is assigned daily pass:	
	(1) Records entry at station	
	(2) Assigned daily pass	
	(3) Chaperoned in computer facility by authorized manager	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	(4) Returns pass and records exit at station	
	g. Deliveries into computer facility:	
	(1) Computer facility employee receiving delivery collects delivered item(s) at station (loading dock)	
	(2) Delivery person allowed to accompany delivery into computer facility	
	If yes, delivery person:	
	(a) Records entry in computer facility register	
	(b) Assigned daily pass	
	(c) While making delivery, monitored by computer facility manager (or manager's designee)	
	(d) Upon completion of delivery, returns pass, and records exit in register	
4.08	Computer facility personnel	
	a. Required to wear company I.D. when in computer room(s)	
	b. Physical access control device assignment recorded in manual or electronic register, and register kept up to date	
	c. Know to challenge persons not wearing appropriate I.D. in computer rooms	
	d. When dismissed or resign or complete tour of duty, required to relinquish computer facility physical access control devices	
	e. When dismissed or resign, required to relinquish company I.D.	
	f. After departure:	
	(1) Names/security devices removed from all systems/authorization lists	
	(2) SWBT entities are notified (some possibilities: building security, mail services, real estate management, vendors the employee has worked with, etc.)	
	(3) Supervisor notifies SUITS administration for I.D. activation	
	g. When departing in anger, escorted from building	
4.09	Vendor	
	a. Assigned unique vendor I.D./interim I.D.	
	b. Vendor I.D./interim I.D. assigned by SWBT, not vendor company	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	c. Must wear vendor I.D./interim I.D. when in computer room(s)	
	d. Vendor I.D./interim I.D. and physical access control device assignment recorded in register	
	e. Registers kept up to date and retained according to local/company guidelines	
	f. When vendor rep departs, vendor I.D./interim I.D. and any computer facility physical access control devices are collected and destroyed, then removed from register/authorization lists	
	g. When vendor rep departs in anger, is escorted from building	
	h. Replacement assigned a new vendor/interim I.D.	
	i. Not allowed to sign in anyone at any company security station	
	j. Not allowed to use vendor company's I.D. to gain access to SWBT facilities	
4.10	Visitor to computer facility	
	a. Assigned daily pass	
	b. Daily pass recorded in register	
	c. Register checked daily and retained according to local/company guidelines	
	d. Required to wear visitor I.D. when in computer room	
	e. Chaperoned when in computer facility	
	f. Upon departure, daily pass collected and recorded in register	
	g. Not assigned computer facility physical access control devices	
4.11	Company employee who is not a computer facility employee	
	a. Required to wear company I.D. when in computer facility	
	b. Chaperoned when in computer room(s)	
	If no, good reason required	
	c. Computer facility physical access control devices assigned to employee only for good reason	
4.12	Visitor under 18 years old	
	a. Can only access computer room(s) as part of supervised tour group	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	b. Chaperoned by sponsoring computer facility employee when in non-computer-room areas of computer facility	
	c. Visit is of short duration (not entire work shift) uness special permission is obtained in advance	
4.13	Cleaning personnel	
	a. Bonded	
	b. Under same controls as vendors with I.D.	
	c. Records kept of assigned I.D.s and computer facility physical access control devices	
4.14	Computer facility tours	
	a. Not conducted	
	b. Conducted in computer rooms, magnetic media operations facilities, or offices. If yes:	
	(1) Approved in advance by management	
	(2) Tour group-to-guide ratio is 7:1 or less	
	(3) Records kept of tour's date-time & member/guide names	
	c. Conducted in magnetic media libraries. If yes:	
	(1) Approved in advance by management	
	(2) Tour group-to-guide ratio is 2:1 or less	
	(3) Records kept of tour's date-time & member/guide names	
4.15	Computer room(s) each have no more than two entry points (major data center's computer room might have three entry points if it includes a magnetic media facility entrance)	
4.16	Data center raised floor computer room entry points are card key protected	
4.17	Magnetic media facilities	
	a. Magnetic media library (or AMA tape library in data center)	
	(1) One entry point only	
	(2) Entry point is card key protected	
	(3) Entry point is combination lock protected (only if entry point opens into magnetic media operations library)	
	b. Magnetic media operations room/library	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	(1) No more than two entry points	
	(2) Each entry point is card key protected	
4.18	Non-data-center raised floor computer room	
	a. One entry point per room. If yes:	
	(1) Card key protected	
	(2) Combination lock protected	
	b. Two entry points per room: card key protected	
4.19	Computer rooms on regular floors, then entry points protected by:	
	a. Card key system; or	
	b. Combination lock; or	
	c. Key lock	
4.21-4.25	Computer room perimeter doors:	
	a. Lock from outside	
	b. If automatic locking, doors have fail-safe locks	
	c. Self-closing	
	d. Remain closed when not in use	
	e. Propped open only during emergencies or materials movement	
	f. If disabled, access/egress immediately controlled	
	g. In addition, for raised floor computer rooms:	
	(1) Doors are alarmed to signal forced entry	
	(2) Alarm(s) audible in local area	
	(3) Alarm(s) tied to central monitoring station	
4.26	Computer room(s) unmanned at times	
	a. Alarm(s) for windows/glass in perimeter doors or walls (optional for building perimeter windows above ground level)	
	b. Alarm(s) audible in local area	
	c. Alarm(s) tied to central monitoring station	
	d. Perimeter door(s) with exterior hinges have welded hingepins or locking screws	
4.27	Building perimeter windows that are part of computer room	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	a. Blinds in place	
	b. Blinds closed except when relieving environmental problem	
4.28	Building elevators used by non-computer-room personnel do not open into computer room(s)	
4.29	C.E. rooms or other vendor rooms do not open into computer rooms	
4.30	Computer facility storage rooms opening into public/semi-public areas are closed and locked when not in use	
4.31	I/O area	
	a. I/O door to computer room locked when not in use	
	b. I/O area that includes computer room entry point: entry point is card-key-controlled	
4.33-4.37	Card key system and administration	
	a. System codes can be added and deleted	
	b. Granted and denied entries and exits are logged	
	c. Area/room access levels can be set for each card key	
	d. Card key holder who cards in must card out	
	e. Emergency power available	
	f. When system malfunctions, it does not lock protected door(s)	
	g. Occurrence of unusually high number of unsuccessful access attempts is investigated	
	h. No one is assigned more than one card key	
	i. Persons issued card key know to:	
	(1) Not loan card key to anyone	
	(2) Immediately report loss of card key	
	(3) Immediately relinquish card key when departing	
	j. System equipment secured when unattended	
4.38-4.42	Combination lock	
	a. Combination different for each functional area	
	b. Combination changed when personnel depart area	
	c. Combination changed quarterly regardless of personnel activity	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	d. If powered by electricity, backup power in place	
4.43	Door key lock numbers, and names of persons assigned keys, logged in journal	
4.44	CCTV	
	a. Cameras monitored when active	
	b. Camera lenses cleaned on scheduled basis	
	c. Camera/system disabled: guard protects scanned area	
4.46	Computer terminals, PCs, or associated printers	
	a. Screens do not display passwords	
	b. Note paper (containing passwords) not posted on device	
	c. Logged off/powered-off after session or screen locks/blanks out	
	d. Located outside computer room	
	(1) Secured when unattended	
	(2) Access by maintenance personnel monitored	
4.47	Hardcopy from terminal/PC printer does not display passwords	
4.50 4.51	Computer facility personnel know to:	
	a. Not publicly post dial-up terminal telephone numbers	
	b. Not accept phone requests for computer system access/authorization information	
	c. Report security breaches to management	
	d. Protect sensitive documents/manuals	
4.52	Colocation (permitting customer floor space in SWBT computer rooms) exists	
	If yes, applicable guideline(s) in SW 007-590-905, Item 4.52 are followed	
4.56	Checking of incoming and outgoing items at security station performed according to O.P. 78 or SW 007-590-911	
4.57	Contingency plan in place to secure facility during civil disturbance	
4.58	After employee evacuation of computer facility, it will be secured	
4.59	Multilevel computer rooms	
	a. Each level has only one entry point	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	b. If no, then if each level must have two entry points, each point is card key protected	
ENVIRONMENTAL CONTROLS		
5.02	All computer rooms are located at or above ground level	
	If no, the computer room(s) below ground level have:	
	a. Sealing and foundation draining devices	
	b. Water pumps available (somewhere in the building)	
	c. Water detection devices/alarms	
	d. No building perimeter windows	
5.03	Computer room perimeter windows are watertight	
5.04	Items that are moisture-sealed:	
	a. Occupied/unoccupied cable holes/slots in slabs/walls	
	b. Shaft enclosures	
5.05 5.06	Air ducts serving other areas:	
	a. Do not pass through a computer room	
	If no, ducts have U.L.-listed fire dampers	
	b. Do not pass through magnetic media facilities	
5.07	Power for computer room lighting and equipment is separate	
5.08	Computer facility has emergency lighting	
5.09	Exposed water pipe in computer room is kept to a minimum	
5.09- 5.11	Water pipe valves and guages:	
	a. Clearly labeled	
	b. Building operations or computer facility personnel on each work shift know location	
5.10	Water pipe for water-cooled equipment in computer room (and for sprinkler system, if applicable) has shut-off valves, check valves, and pressure guages	
5.12	Water removal equipment in place in building	
5.13	Water detection devices/alarms for raised floor computer rooms	
	a. Alarms sound in local area	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	b. Alarms connected to monitoring station	
5.14	Tarpaulins or plastic sheets are available to cover computer equipment	
5.16	Computer facility a/c compressors protected from unauthorized use	
5.17	Drip pans installed on all air handler units	
5.18	Contingency plan in place to handle a/c loss	
5.20	Magnetic media facilities maintain:	
	a. Temperature range of 65-75 degrees Fahrenheit	
	b. Humidity range of 40%-60%	
5.21	Instrument in place to record computer room air temperature and humidity	
5.23	Environmental control alarms	
	a. Sound in local area; or	
	b. Connected to monitoring station (when computer room(s) are unmanned at times)	
5.24	Alarms monitoring electrical power, a/c, and liquid coolants	
	a. Sound in local area; or	
	b. Connected to monitoring station (when computer room(s) are unmanned at times)	
5.25 5.26	EPO switches	
	a. In computer room near main access/egress point(s)	
	b. Activation procedures in place	
5.27	Power rooms and a/c fan rooms locked when unattended	
5.28	Main power cable:	
	a. Running into computer facility building is underground	
	b. Is unexposed when running outside computer facility (but within building)	
5.29 5.30	Computer facility backup power system	
	a. Inspected and tested on recurring basis	
	b. If UPS, batteries are separated from equipment	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
5.31	UPS batteries used in computer room(s)	
	If yes:	
	a. Batteries housed in cabinets/racks	
	b. Batteries are sealed and don't emit gases during charging	
	c. Computer room ventilation capable of filtering possible gas emissions during abnormal battery charging	
	d. Battery cabinets/racks are grounded	
	e. Battery terminals have covers	
	f. Battery connectors (for wiring) have covers or are shielded to prevent accidental contact by people	
	g. Floor-loading adjustments made to accommodate battery weight (optional)	
	h. Battery covers are nonflammable	
	If no, then computer room area where batteries reside is protected by:	
	(1) Gaseous flooding system or sprinklers	
	(2) Smoke/heat detection system	
	(3) Around-the-clock monitoring of computer room by authorized personnel	
	(4) Halon 1211 or comparable fire extinguisher(s)	
	i. Batteries supply emergency power for computers even after EPO switch activation shuts off power to computers	
	If yes:	
	(1) Batteries have separate, dedicated EPO switch	
	or	
	(2) Administrative procedures in place to enable prompt, manual shut-off of power to batteries	
5.32	Valve-Regulated Lead-Acid (VRLA) batteries used (optional)	
	If yes, then recommendations in Advisory Letter (AL) 94/03-001 "Risk of Explosion with Valve-Regulated Lead-Acid Batteries" are followed (copy of AL can be obtained from CSAG)	
5.33	No electrical equipment maintained in magnetic media library	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
5.34	Tape degaussers/evaluators not maintained in close proximity to magnetic media in magnetic media operations library	
5.35	Metal tape/cartridge storage racks are electrically grounded	
5.37	Computer facility checked yearly for contaminants	
5.38	Computer room air plenum and air ducts checked regularly for dust buildup	
5.39	A/C and environmental systems checked on regular basis	
5.40	Critical computer systems (that control a building's environment) have dial-in access	
	If yes:	
	a. Dial-in access control is evaluated periodically	
	b. Token device or dedicated circuits are used	
5.41	Magnets or devices containing magnets are prohibited in computer rooms	
5.42	Bursting and shredding equipment kept out of computer room	
5.44	Building air intakes do not supply computer room(s)	
	If no, then intakes are covered with protective screening and are strategically located to lessen intake of pollutants or debris	
OTHER FACILITY CONTROLS		
6.01	Computer facility not publicly identified as such	
6.01	Building/floor directories do not have signs/listings identifying computer facility's location	
6.02	Manager appointed to administer physical security for facility	
6.03	Physical security manager familiar with SW Section 007-590-905 and SW Section 007-150-100	
6.04	Physical security manager inspects computer room condition-security twice yearly	
6.05	Contingency plan in place to handle computer facility shutdown during emergency	
6.06	Computer facility personnel trained to handle call-in threats	
6.06	Contingency plan in place to handle bomb-terror threats	
6.07	Resident vendor reps required to keep vendor rooms in good order	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
6.08	Computer facility equipment supplies inventory kept up to date	
6.09	Photographing areas or contents of a computer room	
	a. Photographer is neither a minor nor tour group member	
	b. Photographer performs some service for the Company	
	c. Photographer and Company sponsor will agree in advance about what will be photographed and where photo shoot will take place	
	d. If requested, photographer will allow Company sponsor to examine photos, and confiscate originals, copies, negatives, etc., of photos compromising Company proprietary information	
	e. If requested, photographer will sign nondisclosure agreement	
6.10-6.12	Company proprietary documents	
	a. Disposed of according to O.P. 47	
	b. Secured until delivered/mailed	
	c. Document disposal vendor required to sign nondisclosure agreement	
6.15	Special procedures in place to retrieve data from water-contaminated tape cartridges	
6.16 6.17	Defective tapes/cartridges degaussed before destroyed or before returned to magnetic media vendor	
6.18	Disposable disk packs are rendered unreadable when disposed of	
6.19	Magnetic media removed from computer facility is journalled/tracked	
6.20	For magnetic media sent to off-premise storage site:	
	a. Computer facility management makes regular inventory check at off-premise storage site	
	b. Computer facility management makes periodic spot-check to test media readability	
EARTHQUAKE PREPAREDNESS CONTROLS (See Appendix 5 for illustrations.)		
7.02	For computer facilities in buildings located in Zone 3 (all building floors) or Zone 2 (upper 60% of building floors):	
	a. Raised floor computers secured to subfloor by toggle rods	
	b. Raised floor braced by pedestals shot-pinned to subfloor	

COMPUTER FACILITY PHYSICAL SECURITY CONTROLS CHECKLIST

SW905 Sect	SECURITY AREA/REQUIREMENT & COMPLIANCE (Answer YES, NO, or N/A; Explain answers of NO or N/A)	
	c. Computer furniture units (taller than 3 feet) on raised floor are secured to wall or subfloor	
	d. Data communications cabinets with doors:	
	(1) Doors close tightly	
	(2) Doors remain in closed position when not used	
	e. Data communications cabinets without doors: modems secured to cabinet racks	
	f. Computer terminals, PCs, and associated printers secured to work surfaces by velcro fasteners or 3M adhesive fasteners	
	g. Tape cartridges held in cartridge racks by auto pack holders with lips	
	h. Electrical conduit and chilled water attachments anchored by fasteners	
7.02	For computer facilities in buildings located in Zone 2 (lower 40% of building floors):	
	a. Data communications cabinets with doors:	
	(1) Doors close tightly	
	(2) Doors remain closed when not used	
	b. Data communications cabinets without doors: modems secured to cabinet racks	
	c. Computer terminals, PCs, and associated printers secured to work surfaces by velcro fasteners or 3M adhesive fasteners	
	d. Tape cartridges held in cartridge racks by auto pack holders with lips	
	e. Electrical conduit and chilled water attachments anchored by fasteners	