



RELIGIOUS INSTITUTION SECURITY SURVEY REFERENCE MATERIAL AND CHECKLIST FOR PREVENTING BURGLARIES, VANDALISM, TERRORISM, AND OTHER CRIMES

SDPD Crime Prevention

May 31, 2017

This paper contains reference material for security surveys of religious institutions. It deals with security planning and procedures, access control, landscaping, signage, cameras, arson and terrorism prevention, building hardening, etc. The survey checklist is designed for use by the institution or by a SDPD Community Relations Officer (CRO) in your area, who can be called to do a free survey. In this case the officer should do the following to prepare for the survey. Information should be reviewed for the past two years.

- Read the reports of past crimes at your address.
- Review the past calls for service concerning activities at your address.
- Look at past crimes and arrests in your immediate area, e.g., within 0.25 miles of your address.

The officer should also ask the following questions.

- Why did you call to request a survey? Usually this will be because of a recent crime, e.g., a burglary.
- Who else works regularly in and around the institution? This may be a gardener, janitor, pest controller, vendor, etc.
- What contract work has been done recently? This may be carpeting, window cleaning, remodeling, etc.
- How many people work at the institution? Attend worship services? Other activities? Classes?
- Who has keys, gate codes, etc?
- Do you have a burglar alarm? Who has the code? What are your procedures for responding to an alarm?
- Do you have cameras? Where are the monitors? How are they used?

SDPD division addresses and phone numbers are listed below.

Central	2501 Imperial Ave. SD 92102	(619) 744-9500
Eastern	9225 Aero Dr. SD 92123	(858) 495-7900
Mid-City	4310 Landis St. SD 92105	(619) 516-3000
Northeastern	13396 Salmon River Rd. SD 92129	(858) 538-8000
Northern	4275 Eastgate Mall SD 92037	(858) 552-1700
Northwestern	12592 El Camino Real SD 92130	(858) 523-7000
Southeastern	7222 Skyline Dr. SD 92114	(619) 527-3500
Southern	1120 27th St. SD 92154	(619) 424-0400
Western	5215 Gaines St. SD 92110	(619) 692-4800

CONTENTS

SECURITY PLANNING

ACCESS CONTROL

- Fences, Walls, and Gates
- Deadbolt Door Locks
- Single Doors without Deadbolt Locks
- Double Doors without Deadbolt Locks
- Exterior Doors
- Burglar Alarms
- SDPD Access
- Janitor and Other Contractor Employee Access
- Uniformed Guards
- Heating, Ventilation, and Air Conditioning Systems
- Secure or Backup Electrical Power
- Dumpsters
- Parking Lots

LANDSCAPING

SIGNS

CAMERAS

SECURITY PROCEDURES

- Security Checks
- Reporting Vandalism
- Staff ID Badges

PREVENTING VANDALISM

- Graffiti
- Art Vandalism
- Skateboarding

PREVENTING ARSON AND LIMITING FIRE DAMAGE

BUILDING HARDENING

HELP FROM THE SDPD

- Letter of Agency
- Citizen Request Form

EMERGENCY PROCEDURES PLANNING

- Limiting Casualties in Attacks by Active Shooters

REPORTING SUSPICIOUS PERSONS, ACTIVITIES, VEHICLES, ETC. TO

PREVENT TERRORISM

- Emergencies. Call 911
- Non-Emergencies. Call SDPD at (619) 531-2000 or (858) 484-3154
- Other Indicators of Terrorist Activities

SECURITY CHECKLIST

SECURITY PLANNING

Security planning usually involves the following steps:

1. Form a team with people that represent all elements of the institution. The team leader should be the person in charge of security at the institution.
2. Identify assets and people that might be targets of criminals, and review their protection.
3. Estimate the risk to the targets from various threats in terms of the likelihood of a successful attack and the damage that might occur.
4. Define additional countermeasures to protect the targets from various threats.

The plan should include physical crime prevention measures, duties of the staff and hired security guards, and ways members and neighbors can help. Physical measures include lighting, fencing, gates, locks, alarms, cameras, barriers, etc. Staff and security guard duties include patrolling the property, observing people and activities on and

near the property, controlling access by visitors and delivery/service people, educating the members in crime prevention, reporting crimes and suspicious persons and activities, keeping detailed records of crimes and damage to the property, monitoring cameras, handling mail and packages, developing procedures for dealing with problems, etc. There should someone responsible for security present at all times. This person would have the authority to deal with intruders and trespassers, call **911** in emergencies and the SDPD in non-emergencies, order evacuation, etc. It might be the executive director during business hours and others during services, evening programs, special events, etc. Members can help by reporting suspicious persons and activities and providing good descriptions of the people and vehicles involved. Neighbors can also help and should be included in security planning.

Security measures should be considered in layers to provide protection in depth. An outer layer would consist of walls, fences, and gates at the property line to control access to the grounds. A middle layer would consist of gates and doors to the buildings to control access to them. And the inner layer would consist of locked rooms to protect assets and people inside the buildings. Each layer would be designed to delay an intruder as much as possible. This delay should either discourage a penetration or assist in controlling it by providing time for an adequate response. The security functions would be to prevent, deter, detect, delay, assess, and respond.

The security plan should focus on the most likely threats that can cause the most damage. It should also deal with unlikely threats that can be countered simply and inexpensively. Others like armed intruders and active shooters will be difficult and costly to deal with. However they must also be considered these days.

This planning should be carried out by a Safety and Security Committee that would be created in your institution. It would also deal with staff training, security inspections and drills. A comprehensive guide to security planning for religious institutions can be read and downloaded from the Community Security page on the website of Anti-Defamation League (ADL) at www.adl.org/combating-hate/community-security. It is entitled *Protecting Your Jewish Institution: Security Strategies for Today's Dangerous World*. This page also provides access to additional ADL and other security resources. Another good source of information on a variety of security topics is the website of the Secure Community Network at www.scnus.org.

ACCESS CONTROL

Fences, Walls, and Gates

Well-built walls, fences, and gates are the first line of defense against criminals. Unless privacy and noise reduction are needed, open ornamental metal or chain link fences are preferred over solid walls because they do not block visibility into the property or provide hiding places. And they are less susceptible to graffiti. Fences, walls, and gates should be at least 6 feet high.

Chain link fencing should have its bottom secured with tension wire or galvanized pipe, or embedded in concrete. This prevents someone from lifting the bottom of the fence and crawling under it. And to make a chain-link fence more difficult to climb you can install outward-angled “barb-arm” supports on top of the fence posts with strands of smooth wire on them. (No barbed or sharp-pointed wire is permitted in the City except for agricultural uses in agricultural zones per San Diego Municipal Code Sec. 142.0360.) To make wrought-iron fences more difficult to climb the horizontal elements should be located only at the top and bottom on the inside of the fence. And outward-curving pickets can be attached to the tops of the vertical elements.

Wrought-iron gates that are opened on the inside by a lever arm or knob should have shields on them and the adjacent fencing to prevent a person from reaching in to open them. These shields can be solid plastic or metal, or open-metal mesh. Gates with lever-arm locks should also have a cylindrical shield around the arm to prevent a person from opening the gate by inserting a thin wire with a hook at one end through, over, or under the gate to rotate the arm and thus open the gate. Gates with locks that have beveled latches that are visible from the outside should have a latch guard to prevent a person from inserting a thin piece of metal or anything else between the frame and the gate to push in the latch. The guard should be centered on the latch and extend at least 12 inches above and below it. A deadbolt lock would not have this problem, nor would a gate that is secured with a shielded- or hidden-shackle padlock that cannot be drilled out or cut with bolt cutters.

Wrought-iron or chain-link gates that are opened on the inside by a push or press bar should have a solid metal or plastic shield on the inside of the gate that extends at least two feet above and below the bar. The shield should be designed to prevent a person from opening the gate from the outside with a coat-hanger wire that is shaped into a U, inserted through the gate above and below the bar, and pulled against the bar to open the gate. The shield will also prevent a person from reaching in and depressing the bar. Another shield should be installed around the bar to prevent the use of a wire or anything else to depress the bar. The gate should also have a latch guard if it has a visible beveled latch.

All gates should also have springs that close them securely after a person goes through. And they should be alarmed to warn the staff person responsible for security that a gate has been left open. That person would then go and close it.

Deadbolt Door Locks

When a building is unoccupied its exterior doors can use single-cylinder deadbolts that are separate from other locking mechanisms. These locks should have a throw of at least one inch, be key-operated on the outside, and have a thumb turn on the inside. They cannot be used when the building is occupied because California Fire Code Sec. 1008.1.9 states that egress doors shall be readily openable from the egress side without the use of a key or special knowledge or effort. The thumb turn is deemed to require special knowledge. It also requires twisting of the wrist to open the door, which makes it prohibited in the California Fire Code. When a deadbolt is installed a sign must be posted on or adjacent to the door saying **THIS DOOR TO REMAIN UNLOCKED WHEN BUILDING IS OCCUPIED** per California Fire Code Sec. 1008.1.9.3. Deadbolts can also be used on interior doors to individual offices and storage rooms.

Single Doors without Deadbolt Locks

Doors with beveled latches that are visible from the outside should have latch guards that extend at least 12 inches above and below the latches. This will prevent a person from sliding something between the door and its frame to push in the latch.

Doors that are opened on the inside by a push or press bar, i.e., one that rotates downward when pushed, and have a gap between them and their frames can be opened with an L-shaped rod that is inserted next to the bar, turned 90 degrees, and pulled to depress the bar. This can be prevented by attaching a strip of metal or some other material to the door to cover the gap or installing a magnetic lock that can't be fooled by something inserted between the doors. It is better if there is no gap between the door and its frame.

Doors that are opened on the inside by a lever arm and have a gap underneath them can also be opened with a lever-opening tool like the Keedex K-22. This tool has a curved wire that is inserted under the door and raised to hook over the lever arm on the inside of the door. The wire is then pulled to rotate the lever arm downward to open the door. This can be prevented by attaching a threshold strip to the floor under the door and a brush-sweep to on the bottom of the door. They would close the gap and prevent the tool from being inserted.

Doors that are opened on the inside by a press bar and have a gap underneath them can be opened with a lever-opening tool like the Keedex K-22 as described above. Use of a threshold strip and door brush-sweep would close the gap and prevent the tool from being inserted.

Double Doors without Deadbolt Locks

Doors with a post between them and beveled latches that are visible from the outside should have latch guards that extend at least 12 inches above and below the latches. This will prevent a person from sliding something between a door and the post to push in a latch.

Doors that don't have posts between them and don't have latches on their sides should have latches on both their tops and bottoms that go into the tops of their frames and the floor, respectively. Doors that only have latches that go into the tops of their frames can be opened by a person pushing on one door near the floor to create enough space between the doors for a hand to reach in and depress a push bar or press bar on the other door.

Doors that are opened on the inside by push or press bars and have a gap between them can be opened with an L- or T-shaped rod that is inserted between them next to the bars, turned 90 degrees, and pulled to depress one or both bars. This can be prevented by attaching a strip of metal or some other material to one door to cover the gap or installing a magnetic lock that can't be fooled by something inserted between the doors. It is better if the doors have no gap or a post between them.

Doors that are opened on the inside by press bars and have don't have a gap between them but do have one underneath them, can be opened with a lever-opening tool like the Keedex K-22 described above. Use of a threshold strip and a door brush-sweep would close the gap and prevent the tool from being inserted.

Exterior Doors

Exterior doors should be kept locked all the time. Entry by staff people would be by key, fob, card, or keypad code. (Keys or keypads with a single code should not be used because a record of entries by individual staff people cannot be kept.) When each staff person has an individual fob, card, or keypad code it will then be possible to: (1) keep a record of their use, (2) deactivate a fob, card, or code when a person leaves, (3) deactivate a fob or card if one is reported lost or stolen, (4) trace the use of a fob, card, or code to the staff person it was issued to, and (5) restrict their use by day of the week, hours of the day, and period of time.

A video intercom should be installed at the main entrance so visitors, delivery/service people, members, school children and parents, et al can be "buzzed" in after a receptionist or staff person in the lobby observes and talks to them. Signs in the parking lot and outside the building should direct visitors and others to this entrance. Visitors and delivery/service people would be logged in and receive a visitor badge. For added security they might be required to show a photo ID. They should also be escorted while in the building and sign out when leaving.

Measures are also needed at all exterior doors to prevent them from being propped open for reentry or unauthorized entry, but still open quickly from the inside in an emergency. These include an audible alarm to warn the staff person responsible for security that a door is open, alarm-activated cameras, and delayed-egress hardware. A control panel should be installed in the lobby or security office to show the status of all exterior doors and interior doors to rooms or areas that are normally kept locked.

Institutions with multiple buildings should be fenced and gated. Access by people and vehicles should be controlled at the exterior gates.

For institutions that believe it is more important to be open and welcoming than secure, there should still be a main entrance. Its door would be open when a receptionist or staff person is there to greet visitors. That person should have access to silent alarms to call for help in dealing with a threat from someone entering the building and to warn other staff people of a threat.

Burglar Alarms

Install a good alarm system. One will usually include one or more of the following components: magnetic contacts on doors and windows, photocell or pressure sensors with annunciators at unlocked or open doors, heat or motion detectors in interior spaces, glass break detectors, keypads with a means of checking the status of the system, and audible alarms. All equipment should be Underwriters Laboratories (UL) certified.

- Multiple sensors are preferred because they reduce false alarms, which are wasteful of police resources and lead to fines and permit revocation.
- See San Diego Municipal Code (SDMC) Secs. 33.3701-33.3723 for burglary alarm business and agent requirements and responsibilities, alarm-user permit requirements, etc. Call SDPD Permits and Licensing at **(619) 531-2250** about obtaining an alarm permit.
- Get alarm company references from other businesses. Get at least three estimates in writing. The SDPD does not prefer or recommend companies, brands, or types of security systems.

- Make sure the alarm company has a City Business Tax Certificate and is licensed by the California BSIS. You can verify the latter by calling **(800) 952-5210** or going online at **www.bsis.ca.gov/forms_pubs/online_services/verify_license.shtml**.
- If your system is monitored, make sure the monitoring station is open 24/7 and has backup power. The company's customer service department should also be open 24/7.
- Make sure you understand your service contract, all the points of protection and the equipment to be installed, the initial and monthly payments, and the warranty period.
- Inform your insurance company. You may qualify for a discount.
- Harden the telephone line that sends the alarm signal to the alarm company so it cannot be cut from the outside. And if it is cut, have the system send an alarm to the alarm company. If the telephone line is contained in an outside box, the box should be alarmed or locked with a shielded- or hidden-shackle padlock. Or the system could have a wireless backup that would send the alarm if the telephone wire is cut.
- The system should also have a fail-safe battery backup. Check the batteries periodically and replace them if necessary.
- Test the system periodically to make sure it works properly. Have it inspected and checked at least annually.
- Develop procedures for turning the alarm on and off to avoid false alarms. The last person to leave should turn the system on and the first person to arrive in the morning should turn it off. Then when others come in at night or on days when the institution is closed they will have to turn the system off when they enter and on when they leave.
- When an alarm occurs the alarm company will call your institution or a person designated to receive the call. It will call to report the alarm if it gets no answer, the person answering the call does not have the correct codeword(s), or the person answering the call has the correct codeword(s) and says to call to report the alarm. The responding officers will check for a sign of a forced entry. If none is found and all the doors are locked, they will leave. They will not enter the building. In the meantime the alarm may still be going off and the burglars may still be inside. To prevent this someone from your institution or your alarm company also needs to respond to the alarm call. If that person arrives before the officers, he or she should wait for them to arrive and then let them in to investigate the alarm. (He or she should not go in alone because the burglars may still be inside.) If he or she arrives after the officers have left, the officers can be called to return. Alternatively, if your alarm company provides a response service it should be given a means of getting into your building so it can investigate the alarm or wait for officers to arrive and let them in to conduct an investigation. In any case, someone from your institution should respond to all alarm signals. Don't assume a signal is a false alarm. Burglars could be testing or interfering with your line. Never let alarm signals, telephone trouble, or other disturbances go unexplained.
- If provisions have been made for SDPD access when no one is present to let them in as suggested below, responding officers will be able to enter the building to investigate an alarm. Someone from your institution should still respond to the alarm call.

SDPD Access

SDPD access is especially useful in dealing with after-hours burglaries when there is no sign of a break-in and no one is present or en route to let the responding officers in. Officers will need to enter the institution to investigate the cause of the alarm. Often burglars enter with a fob or card, or are let in by someone working there, e.g., a janitor, and leave no sign of break-in. With no access and no signs of a break-in, officers will leave the scene.

If the entry system has backup power, which would be needed in the event of a power failure to keep it operational, SDPD access can be provided with a numerical keypad or a telephone-entry system. An entry code would be given to the Department for use at entry gates and building doors. It would be stored in the SDPD's computer system and transmitted in dispatch messages to officers who need to enter the institution. The institution's executive director should call the CRO in the SDPD Division that covers the institution to have the code entered in the SDPD's Premises Information (PIN) file. Division addresses and phone numbers are listed on the first page of this paper.

If the entry system does not have backup power, officers will need a key to open the gates and doors. One should be given to the CRO to be put in a fence- or wall-mounted combination lock box that would be located near the main entry gate and building doors. (This box would be similar to the Knox box used by the San Diego Fire-Rescue Department.) The combination of the box would be stored in the SDPD's PIN file and transmitted in dispatch

messages to officers who need to enter the institution. Officers would open the box, remove the key, use it to enter the institution, and return the key to the box when they leave. In this case a code for the telephone-entry system would not be needed.

Once officers enter the institution they will need to go straight to the location of the problem. For this maps with a YOU ARE HERE reference point should be posted at the entrances where officers will be sure to see them. The map should show all buildings, elevators, stairways, offices, activity rooms, parking lots, play areas, etc.

Janitor and Other Contractor Employee Access

Religious institutions should be concerned about the loyalty and honesty of all persons working in their facilities, e.g., janitors, gardeners, equipment technicians, etc. In selecting any service contractor you should check its references and make sure it is insured and bonded. Insurance will protect you from damage caused by the contractor's employees. A surety bond will guarantee that the work will be performed as stated in the contract. For janitorial contractors you can require a janitorial services bond that will cover theft or other losses resulting from dishonest acts committed by an employee acting alone or in collusion with other persons. Some bonds require that the employee be prosecuted and convicted of the crime. Others require evidence of employee dishonesty. The conditions for coverage would be negotiated in drafting the bond.

You should also check that the contractor is licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. This can be done on the Master Business Listing page of the City's website at www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml. Construction contractors should be licensed by the State of California. You can check the status of a contractor's license on the Contractors State License Board's website at www2.cslb.ca.gov/OnlineServices/CheckLicenseII/CheckLicense.aspx.

You can also require that the contractor conduct a background investigation on each employee that will work in on the contract. For this you will need to specify the following: (1) information an employee will have to provide, e.g., personal history, references, fingerprints, etc., (2) kinds of checks to be made, e.g., employee's name and Social Security Number (SSN), criminal history, Department of Motor Vehicles (DMV) record, credit record, civil action history, etc., and (3) criteria for passing each check, e.g., no criminal convictions or outstanding warrants, no bankruptcies, no civil judgments, etc. The contractor should also be prohibited from substituting a cleared employee with one that is not cleared, or subcontracting any of the services.

The opportunities for employee theft can be reduced by having the contract work done during normal business hours. If it is done after hours, as with most janitorial services, the contractor's employees should have unique access codes or cards for the building, office suite, alarm system, etc. This will provide a record of when the employees enter and leave these areas.

Uniformed Guards

In hiring private security you would deal with a Private Patrol Operator (PPO). This person or company must be registered with the California Bureau of Security and Investigative Services (CBSIS) and have a PPO license, for which there are many requirements. The PPO would provide Security Guards for the security services. Security Guards must also be licensed by the CBSIS. They will need to pass a criminal history check and complete a 40-hour training course.

Heating, Ventilation, and Air Conditioning Systems

Conduct an inspection of your system to determine whether it can become an entry point for hazardous contaminants, particularly chemical, biological, and radiological agents. Components at ground level may be especially vulnerable. See *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, Publication 2002-139 dated May 2002 by the National Institute for Occupational Safety and Health (NIOSH) of the U.S. Department of Health and Human Services for some recommended actions. It can be read on the NIOSH website at www.cdc.gov/niosh/docs/2002-139.

Secure or Backup Electrical Power

Because lights and other security systems work on electrical power it is important that measures be taken to prevent disruption of exterior power or provide interior backup power. At a minimum, exterior circuit breakers should be installed in a sturdy metal box that is locked with a shielded- or hidden-shackle padlock.

Dumpsters

Outside trash enclosures should be screened with a minimum 6-foot-high solid screening enclosure and be located in the open or next to a wall or another structure where there is either good visibility of the space behind it or no space behind it that can be used as a hiding place. The enclosure doors should be locked except when the containers in it are being filled or emptied. If the enclosure doors are not locked, the dumpsters should have bars over their lids that can be padlocked to prevent them from being opened except by the trash removal company. The lids would have an opening through which material can be put in but not taken out. This is to prevent scavenging. The dumpsters should also have signs saying that unauthorized collection of refuse or recyclable material is prohibited per SDMC Sec. 66.0402.

Parking Lots

Parking lots should be well lighted, fenced, and have a single gated or chained vehicle entrance/exit that would be locked at night when the institution is closed. Overnight parking should be prohibited. The entrance/exit can be kept open during the daytime when no terrorist threat alerts have been issued by the U. S. Department of Homeland Security (DHS). However, when services and other events that attract large crowds are held, a staff person, member, or security guard should be posted there to screen vehicles entering the lot.

For those times when the gate is locked during business or school hours, a video intercom should be installed to admit visitors and people entering to drop off or pick up school children. Entry and exit by staff people would be by their fobs, cards, or keypad codes.

LANDSCAPING

Tree canopies should be maintained at least 8 feet above the ground. Bushes should be trimmed to less than 3 feet except where privacy or environmental noise mitigation is a primary concern, or where higher plants would not block any views or light, or provide hiding places. For example, trees with lower canopies could be planted next to a blank wall or the side of a building.

Trees should be planted away from walls, fences, and buildings so they cannot be used to enable someone to climb over or onto them. They should also be planted away from light poles and fixtures so they do not block any light and from cameras so they do not block their fields of view. Bushes along building walls should be trimmed or located far enough from the walls so that a person walking around the building can see that nothing is hidden next to the building.

SIGNS

Signs in the parking lot and outside the building(s) should direct visitors, delivery/service people, et al to the main entrance with the video intercom. Other signs outside should prohibit trespassing, loitering, public parking, etc. and cite the applicable California and SDMC sections.

- NO TRESPASSING signs on private property should cite Cal. Penal Code (PC) Sec. 602. If you file a Letter of Agency with the SDPD as suggested below, you can post NO TRESPASSING signs stating that. The sign would have the address of the property, the name and phone number of the property owner or manager, and the non-emergency SDPD phone number to report suspicious activities. That number is **(619) 531-2000** or **(858) 484-3154**. The signs should be at least 18 by 24 inches in size, have a font visible from the nearest public street, not be accessible to vandals, and be posted on the entrances and spaced evenly on the boundaries of the property. A sample sign is available by clicking on View a Sample Sign on the Forms page of the SDPD website at www.sandiego.gov/police/forms/forms.

- NO LOITERING signs on private property should cite PC 647(h). In this subdivision "loiter" means to delay or linger without a lawful purpose for being on the property and for the purpose of committing a crime as opportunity may be discovered.
- NO LOITERING signs about any school or public place at or near which children attend or normally congregate should cite PC 653b.
- Signs stating that public parking is prohibited and that unauthorized vehicles will be removed at the owner's expense must contain the telephone number of the local traffic law enforcement agency, and the name and telephone number of each towing company that is a party to a written towing authorization agreement with the property owner or manager. The SDPD number for towing impounds is **(619) 531-2844**. These signs must be displayed in plain view at all entrances to the property. They must be at least 17 by 22 inches in size and have lettering that is at least one inch high. These sign requirements are specified in California Vehicle Code Sec. 22658(a)(1), which should be cited on the sign.
- Signs stating that unauthorized vehicles parked in designated accessible spaces not displaying placards or special license plates issued for persons with disabilities will be towed away at the owner's expense, must also contain the address where the towed vehicles may be reclaimed or the telephone number of the local traffic law enforcement agency. The SDPD number for towing impounds is **(619) 531-2844**. Other requirements for these signs are specified in California Vehicle Code Sec. 22511.8.
- The wording on signs regarding cameras is suggested below.

CAMERAS

Cameras are usually used just to record persons and activities in their fields of view. They can be wired or wireless. They can record continually, when motion is detected, at specified times, or on an alarm. After a crime occurs the imagery can be reviewed for usable evidence. Any camera system that is installed should be designed to provide high-quality, color imagery of persons and activities on the premises in any lighting condition for use by the SDPD in investigating crimes. And it should have backup power for at least 12 hours in the event of a power failure. Camera imagery should enable clear and certain identification of any individual on the premises. Its recordings should be kept in a secure place for at least 30 days.

Cameras can be analog or digital, viz. closed-circuit television (CCTV) or Internet Protocol (IP). Imagery from both can be stored and monitored on site and viewed remotely over the Internet. Camera imagery can be used in several ways. In one, recorded imagery is stored for use in future crime investigations. In another, imagery is used as it is being recorded to report and deal with crimes in progress. However, because it is unrealistic to expect someone to monitor cameras all the time, the monitoring might be done at random times or when an alarm or alert condition occurs. Monitoring at random times is usually adequate for dealing with crimes that exist for several hours, e.g., illegal lodging on a sidewalk. Monitoring when an alarm or alert condition occurs is necessary for dealing with crimes that could occur at any time and last a few minutes, e.g., a burglary or a robbery.

Alarms can be triggered by a break-in, motion in an area covered by cameras, an open door or gate, a robbery, etc. Either CCTV or IP cameras can be used to record on alarms. Alert conditions include motion in and out of an area, an unattended object, irregular motion, objects that have moved or are missing, overcrowding, behavior, e.g., casing or tailgating, etc. Programmable IP cameras with video-analytics software, so-called "smart" cameras, are needed to record when specific conditions occur. They have other advantages over CCTV cameras. These include higher resolution, better video quality, and video encryption.

If the building has a burglar alarm, the imagery from CCTV or IP cameras can be accessed over a secure, password-protected Internet link to the alarm company so personnel there can look at the imagery and see what is happening. Or it can be transmitted to a web-enabled mobile device. If a crime in progress is seen, **911** would be called and the dispatcher given the details. This will lead to a higher call priority and a faster response than would occur for an unverified alarm call. Also, the dispatcher can relay real-time information to officers en route to the building. This will enable them to make better, more-informed tactical decisions in dealing with the suspects. Officers might even arrive in time to arrest them.

For activities that don't trigger alarms, "smart" IP cameras can be used to record unusual or suspicious activities in various places in and around the building. Those activities can be defined by various alert conditions that can be set

by day of the week and time of the day. When an alert condition occurs, the imagery would be viewed to see what's happening so appropriate actions can be taken.

In either case, if something suspicious but not a crime in progress is seen, it should be reported to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**.

Because cameras are susceptible to damage by criminals attempting to hide their actions, measures should be taken to make them less vulnerable. Here are some possibilities.

- Mount cameras on high sturdy poles.
- Use damage-resistant cameras.
- Use armored conduits for electrical cables.
- Install cameras where they are within the field of view of at least one other camera.
- Include measures to detect lens blockage and other tampering.

Signs regarding cameras should be posted in order to deter crimes. If they are not monitored all the time, signs should use words like **RECORDED VIDEO SURVEILLANCE IN USE** or **ALL ACTIVITIES ARE RECORDED TO AID IN THE PROSECUTION OF CRIMES COMMITTED ON THE PREMISES**. Don't use words like **SECURITY, PROTECTION, or MONITORING** because they can give people a false expectation of an immediate security response when an incident occurs or that they and their property are somehow being protected by the cameras.

SECURITY PROCEDURES

Security Checks

Staff people should be alert at all times for objects that are not in their proper places, e.g., backpacks, and that nothing unusual has been left unattended. They should check their work areas at the end of each day to make sure that everything is in its proper place and that nothing unusual has been left out. Then they should check their work areas when they arrive the next day to make sure that nothing has changed. They should also be alert for people casing or loitering near the institution during the day.

The first staff person on the grounds in the morning should conduct a walk-around to check for any suspicious objects, vandalism, vehicles in the parking lot, evidence of trespassing or tampering with locks, etc. As discussed in the last section of this paper, the SDPD should be called immediately if any suspicious objects or vehicles are found. Such objects should not be touched or moved. The last staff person on the grounds in the evening should conduct a walk-around to make sure that the alarms are set and that all doors and gates are locked. Any vehicles left in the parking lot should be towed.

Reporting Vandalism

Graffiti vandalism in progress is considered an emergency and should be reported by calling **911**. The person observing the vandalism should not try to stop it but should get good descriptions of the vandals and any vehicles they might have. Vandalism after it occurs should be reported by calling the SDPD's non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Then graffiti should be photographed and removed as soon as possible and any discarded paint cans, etc. should be picked up without leaving fingerprints and saved for the investigating police officers. This will discourage further vandalism. The graffiti should be covered with matching paint so a "canvas" is not left for the vandals.

Graffiti vandalism can also be a hate crime. If any writing threatens or takes credit for acts of domestic terrorism, e.g., arson by the Earth Liberation Front (ELF), Animal Liberation Front (ALF), or anarchists (A), it should also be reported to the SDPD Criminal Intelligence Unit at **(619) 525-8422** so you can get an e-mail address to send the picture to. To educate your staff on hate crimes, including extremist symbols, logos, and tattoos, see the *Hate Symbols Database* under Combating Hate on the ADL website at **www.adl.org/combating-hate**. Also see the California Attorney General's pamphlet entitled *Preventing Hate Crime: What We Can Do!* at **http://ag.ca.gov/civilrights/pdf/HC_English.pdf**.

And if the graffiti appears to be gang related, call the SDPD Graffiti Strike Force at **(619) 531-2890** to get an e-mail address to send the picture to.

Staff ID Badges

Issue photo-ID badges to all staff people and teachers. They should be worn everywhere. They can also be designed for use in card readers to provide access to staff people, as suggested above.

PREVENTING VANDALISM

Graffiti

Graffiti-resistant paint or anti-graffiti coatings should be used on the sides of the building and any other design features that could be vandalized. The San Diego Park and Recreation Dept. specifies the use of anti-graffiti materials manufactured by Monopole Inc. Four coats are applied. The first is Aquaseal ME12 (Item 5200). The second is Permashield Base (Item 6100). The third and fourth are Permashield Premium (Item 5600 for matte finish or Item 5650 for gloss finish). Additional protection can be obtained by planting vines, bushes, etc. along walls and the sides of the buildings. They cover areas that might otherwise be vandalized. However, the landscaping should not be so dense that it provides a hiding place for a bomb next to a building.

The outside of the buildings should be well lighted at night, especially areas that might be vandalized. Cameras could be installed to cover these areas.

Art Vandalism

Sculptures and other works of art should be designed to be resistant to vandalism and easy to repair if it is damaged. Stained glass windows can be shielded by a protective film that prevents them from being broken by thrown objects.

Skateboarding

Physical damage from skateboarding is a serious problem along sidewalks, or steps, and in parking lots. In addition to posting signs prohibiting skateboarding, various design measures should be taken to discourage it. These include:

- Rough ramp and pavement surfaces, especially in front of benches, planter boxes, low walls, steps, and railings
- Pavement cutouts instead of raised planter boxes for trees and bushes
- Small metal or plastic discs or strips on the edges of benches, planter boxes, and other flat surfaces that skateboarders abuse
- Small metal discs or bolt heads on tops of railings
- Height variations, arm rests, or seat dividers on the tops of seating surfaces
- Breaks, bumps, or height variations on low walls, curbs, and planter boxes

PREVENTING ARSON AND LIMITING FIRE DAMAGE

Conduct a survey to identify ways intruders or vandals could start fires. Estimate the possible damage and determine how to prevent or limit it. Get help from the San Diego Fire-Rescue Department (SDFD). Keep in touch with the SDFD and SDPD. Provide them with site plans that show where all facilities are located.

The following physical measures should be taken in addition to those taken to prevent burglary, trespass, theft, and other kinds of vandalism, i.e., fences, gates, locks, lighting, cameras, alarms, security grates or screens, low landscaping, etc.

- Install films or protective shields on windows to prevent firebombs from being thrown into a building.
- Keep rooms and areas with combustible materials locked when not in use or occupied.
- Store combustible materials in a locked room or shed.

- Locate trash enclosures away from the building and keep them locked.
- Remove any signs that indicate when the institution will be closed.

The following surveillance measures can help deter arson and provide early warning of any attempts.

- Meet neighbors and educate them in recognizing unusual activities. Ask them to keep an eye on the property and note any suspicious activities or people in the area. Ask them to record descriptions of vehicles, including license plate numbers, and detailed physical descriptions of people, and to report them to the institution's security officer or the SDPD.
- Participate in local Neighborhood Watch program.
- Have a security guard or staff person on the property at all times. Their duties should include watching for any suspicious activities or people on or near the property, and recording descriptions of vehicles and people.
- Develop a plan for members to drive by and check on the property at random times on a daily basis.
- Be especially aware of people carrying containers that could hold liquid fire accelerants.
- Have persons making security checks on the property remove and secure any fire hazards.

The following measures can help limit damage and help in recovery in the event of a fire.

- Install smoke and fire alarms, and a fire suppression sprinkler system. Connect the fire alarm to a central monitoring station or directly to the fire department. Test batteries at least once a month. Replace batteries at least once a year.
- Locate fire extinguishers at designed locations on the property. Make sure the staff knows where they are.
- Locate hoses at exterior faucets.
- Train staff in use of fire extinguishers and hoses.
- Remove all potential fire hazards from the property, i.e., trash, lawn clippings, debris, etc. Do not store gasoline or flammable chemicals.
- Remove carpeting and mats outside of doors. These can absorb fuel and act as wicks.
- Duplicate all documents, computer disks, and records that are stored on the property. Keep copies elsewhere.
- Keep an inventory of all furniture, equipment, etc., including serial numbers. Photograph or videotape all valuables.
- Reevaluate insurance of buildings and contents annually.

HELP FROM THE SDPD

Letter of Agency

Institutions in the City of San Diego should file a Letter of Agency with the SDPD division that covers their location. This authorizes the SDPD to act as your agent and enter your property to ask unauthorized persons to leave the property; and if they refuse to do so or return thereafter, to enforce any law violations on the property. To do this you should talk to the CRO in your area about filing a Letter of Agency. The form for this Letter must be filled out on the SDPD website in the following steps and filed by clicking on Email Form on the bottom left. You can skip the first step if you know what SDPD Division covers your property.

1. Go to www.sandiego.gov/police/pdf/2013policecitywidemap.pdf to find out what SDPD Division covers the neighborhood in which your property is located.
2. Go to the Forms page on the SDPD website at www.sandiego.gov/police/forms/forms and click on Trespass Authorization/Letter of Agency Form.
3. Click RESET FORM to get the start and expiration dates. The Letter must be renewed every 12 months.
4. Use the drop down menu to enter the Police Division.
5. Fill in the blue blanks on the form.

Citizen Request Form

In addition to filing a Letter of Agency as described above, an institution facing continuing crime problems on its property can submit a Citizen Request Form by going to the Forms page on the SDPD website at

www.sandiego.gov/police/forms/forms, clicking on Citizen Request Form, filling out the Form online with as much information as possible about the problem, and then clicking on the Submit Request button at the bottom of the Form. You can use this Form to request additional patrol and/or to report criminal activity at a specific address. It will be sent to the responsible Division for review and response as appropriate.

EMERGENCY PROCEDURES PLANNING

All institutions should have an emergency procedures manual in addition to a security plan. It would contain the usual procedures for dealing with fires, earthquakes, and medical emergencies, as well as procedures for dealing with the following crime emergencies: telephone bomb threat; telephone chemical or biological threat; suspicious envelopes, packages, and deliveries; armed intruder or trespasser; active shooter; vandalism in progress; robberies; burglary in progress; suspicious persons, objects, activities, and vehicles; terrorist threats; child abduction; bullying; etc. While your manual is still in a draft form you should show it to the CRO in your area to make sure your procedures are consistent with those of the SDPD. After that the manual should be reviewed and updated periodically.

A template for an emergency procedures manual is available from SDPD Crime Prevention by calling **(858) 523-7049**. It was developed for a hypothetical institution with a building, parking lot, and surrounding grounds. Another way to create a manual is to use one of a similar institution as a guide. An Internet search will yield manuals for many different kinds of institutions.

A planning guide tailored to religious institutions was published by the Federal Emergency Management Agency (FEMA) in June 2013. It is entitled a *Guide for Developing High Quality Emergency Operations Plans for Houses of Worship* and can be downloaded at www.fema.gov/media-library/assets/documents/33007. Planning in it is considered in the following steps:

1. Form a collaborative planning team
2. Understand the situation
3. Determine goals and objectives
4. Identify courses of action
5. Prepare, review, and obtain approval of the plan
6. Implement and maintain the plan

The resulting plan would have several functional annexes that deal with evacuation, lockdown, shelter-in-place, recovery, security, threats, and hazards. The guide also takes a closer look at planning for, preventing, and responding to active shooter situations.

Institutions that also operate a school should see the FEMA *Guide for Developing High-Quality School Emergency Operations Plans* dated June 2013 for planning considerations specific to the school environment. It is online and can be downloaded at www.fema.gov/media-library/assets/documents/33599#.

Limiting Casualties in Attacks by Active Shooters

The DHS paper entitled *Active Shooter How to Respond* provides a great deal of useful information on how to respond when an active shooter is in your vicinity, what to do when law enforcement arrives, how to train your staff for an active shooter situation good reference, etc. It can be downloaded from the DHS website at www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf. Additional material is available on the DHS website page on active shooter preparedness at www.dhs.gov/active-shooter-preparedness. It includes the following.

- Active Shooter: What Can You Do
- Active Shooter Webinar
- Active Shooter Workshop Series
- *How to Respond* Resource Materials
- *Options for Consideration* Active Shooter Training Video
- Conducting Security Assessments: A Guide for Schools and Houses of Worship Webinar

The following measures can help protect people in buildings from active shooters.

- Install metal detectors at entrances.
- Install panic alarm buttons that would tell the building's burglar-alarm company to call **911** immediately and report an armed intruder or active shooter. It would only be used in these situations. The alarm company would be told not to call back to verify the alarm.
- Install a rapid emergency response communication system that will contact law enforcement and alert building occupants to take precautions immediately.
- Install doors or shutters in hallways and other places that can be closed and locked remotely to limit the movement of shooters in the building.
- Install cameras that can follow shooters through the building.
- Develop evacuation plans.
- Designate good hiding places for people who don't evacuate.
- Keep office doors locked.
- Provide rooms with strong doors and locks that cannot easily be breached by active shooters.
- Plan how to barricade doors. Locate desks, bookcases, etc. near doors for use as barricades.

BUILDING HARDENING

Only a few things can be done to limit bomb damage to existing buildings, especially if the bomb explodes in or near the building. Films can be applied to windows to reduce injuries from flying glass fragments or drapes can be installed to catch these fragments. Bollards or planter boxes can be installed at building entrances to prevent a vehicle from driving in. And blast-resistant walls can be installed between the building and the adjoining streets and the parking lot.

However, many things can be done to limit damage and casualties in the design of new buildings. Some examples are listed below.

- Use laminated, tempered, or wired glass, plastic acrylics, or polycarbonate sheets in windows. Or attach a safety and security film to the inside of standard glass windows which shatters easily when hit with blast wave. Flying glass then becomes lethal to people inside. Another way to protect people is to hang blast curtains on windows to catch flying glass shards.
- Install bollards or planter boxes at the building entrances to prevent a vehicle from driving in.
- Make building walls blast-resistant.
- Build blast-resistant walls between the building and adjoining streets and parking lots.
- Set the building far back from the adjoining streets and parking lots.
- Install gates or barriers on entry driveways to stop incoming vehicles for inspections.
- Install chicanes in entry driveways to slow vehicles down.
- Locate meeting and conference rooms in the middle of the building and not on the ground floor. People there will be more likely to survive explosions outside the building.
- Eliminate long hallways, spiral staircases, and towering atriums in building design.

These design measures are based on material in the following documents and other sources.

- *Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients*, The American Institute of Architects, 2001. It is online at www.aia.org/aiaucmp/groups/aia/documents/pdf/aiab086647.pdf.
- *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks: Providing Protection to People and Buildings*, Federal Emergency Management Agency, FEMA 427, December 2003. Online at www.fema.gov/pdf/plan/prevent/rms/427/fema427_cvr-toc.pdf.
- *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks: Providing Protection to People and Buildings*, Federal Emergency Management Agency, FEMA 427, December 2003. It is online at www.fema.gov/pdf/plan/prevent/rms/427/fema427_cvr-toc.pdf.

REPORTING SUSPICIOUS PERSONS, ACTIVITIES, VEHICLES, ETC. TO PREVENT TERRORISM

First and foremost, continue with your daily activities. Terrorism is only successful when it disrupts the lives of the people and organizations whose government is targeted. Prepare as you would for any emergency, such as an earthquake. Have a reaction and recovery plan for various scenarios. Go to the FEMA website at www.ready.gov where you can search for more information about threats and planning.

The DHS a public awareness campaign entitled *If You See Something, Say Something*. Its purpose is to encourage the public to contact local authorities if they see suspicious activity. It emphasizes behavior rather than appearance in identifying suspicious activity. Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations, e.g., an unattended backpack in a public place or someone trying to break into a restricted area, rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with federal agencies.

For this you should be vigilant and aware of your surroundings and report anything that doesn't fit in or seems out of the ordinary. Be aware yet fair. Avoid stereotyping and profiling. Some examples of persons, activities, vehicles, etc. that could be considered suspicious are listed below. Some are clearly emergencies. They should be reported immediately by calling **911**. Others may be considered as non-emergencies. They should be reported to the SDPD at **(619) 531-2000** or **(858) 484-3154**. It will notify and coordinate actions with the FBI and other government agencies. When a terrorist act appears imminent you should also notify any law enforcement or security personnel that are in the immediate area. If there is any doubt as to whether the situation is an emergency it is always better to be on the safe side and call **911**.

The ability of the police to locate and arrest criminals often depends on the thoroughness and accuracy of the report you submit. The following information checklist should be used for reporting both emergency and non-emergency crimes:

- Type of activity
- Location: exact street address and nearest cross street
- Time of activity
- Weapons involved
- Vehicle information: activity, direction of travel, license plate, color, make/model, unusual characteristics (e.g., dents, bumper stickers, graphics, wheels, tinted windows, lifted/lowered), cargo type/covering, number of persons, etc.
- Suspect information: activity, direction of escape, race, gender, age, height, weight, weapon type, hair (color, length, style, facial), clothing color and type (hat, tie, coat, shirt, trousers), other characteristics (e.g., tattoos, scars/marks, complexion, missing teeth, scars, glasses), etc.

Remember the five “**W**”s when reporting suspicious activities: (1) **What** is happening? (2) **Who** is doing it? (3) **Where** is it taking place? (4) **When** did you observe it? and (5) **Why** is it suspicious?

Emergencies. Call 911

Emergencies include crimes that are in progress or about to happen, and ones that have resulted in serious personal injury, property damage, or property loss. They also include situations in which the suspect may still be at the scene and various kinds of suspicious activities. By calling **911** you will be linked to the appropriate police as well as fire fighting, medical, and ambulance services. You don't need money to call **911** from a pay phone.

When reporting an emergency be prepared to give an accurate description of what your emergency is and your location, especially if you are calling from a mobile cellular phone. Even if you have an E911-ready cell phone that provides location information based on a Global Positioning System (GPS) and your phone has been activated to work in that capacity, the emergency response will be faster if you provide your location. Otherwise the dispatcher can determine the street address and apartment or condo unit only if you are calling from a landline. Thus, if a landline is available it is always better to use it instead of a cell phone. If you are calling from a gated community or

a controlled-access building, be sure to give the dispatcher the gate or door access code. Answer the dispatcher's questions about the emergency and don't hang up until you are told. With just the address, if the line is disconnected or you cannot speak, an officer will still be dispatched. The following are considered emergencies for reporting purposes.

Persons doing the following:

- Sketching, taking notes, drawing maps or diagrams, photographing, videotaping, or otherwise monitoring facilities not normally associated with tourist activity or other places that may be targets for terrorist attacks, e.g., key government facilities, airports, bridges, chemical plants, power plants, schools, religious institutions, shopping centers, etc.
- Collecting detailed information on facility entrances, exits, driveways, parking spaces, etc.
- Using binoculars, high-magnification lenses, or night-vision or thermal-imaging devices in observing a facility or activity that may be a target
- Attempting to obtain information about a person, place, operation, or event that may be a target
- Attempting to improperly acquire explosives, detonators, timers, weapons, ammunition, body armor, propane bottles or tanks, etc.
- Attempting to buy or rent large trucks or SUVs with cash or without appropriate licenses or vehicle-class endorsements while being unduly nervous or evasive about the use of the vehicle.
- Attempting to buy large amounts of high-nitrate fertilizers or other unusual chemicals
- Loading vehicles with weapons or explosives
- Attempting to improperly acquire official uniforms, passes, badges, IDs, license plates, vehicles, etc.
- Seeking treatment for chemical burns or missing hands/fingers
- Having untreated chemical burns or missing hands/fingers

Objects in the open, or in vehicles or buildings having the following characteristics may be bombs:

- Unattended bags, backpacks, boxes, etc. near places that may be targets
- Having antennas, batteries, timers, capped pipes, etc.
- Emitting a strong chemical odor

Vehicle fires may indicate a failed or misfired explosive device in the following situations:

- The vehicle is parked near a critical infrastructure facility, government building or office, transportation node, or in an area of high pedestrian traffic
- A vehicle occupant is seen fleeing the scene or behaving suspiciously before the fire occurs
- The fire is in the passenger compartment or trunk instead of the engine compartment
- Sparking, flashing, or popping sounds come from the vehicle
- Unusual odors come from the vehicle

Persons, not just adult males, with several of the following characteristics may be suicide bombers carrying bombs.

- Are nervous, sweating, or mumbling
- Are wearing loose or bulky clothing that is inappropriate for the current weather conditions
- Are wearing an inordinate amount of perfume, cologne, or other scents that may be used to mask chemical odors
- Do not look like they belong in the uniform or dress they are wearing, which may be a disguise to elude detection
- Are carrying or wearing heavy objects
- Holding a bag or package close to his or her body
- Are repeatedly patting upper body or adjusting clothing
- Keeping one or both hands in pockets or close to his or her body, possible holding a detonator switch
- Having visible wires or an explosive belt protruding from under his or her clothing
- Having bulges or padding around the midsection
- Appearing well-groomed but wear sloppy clothing

- Having a pale face from recently shaving a beard
- Not responding to direct salutations or authoritative commands
- Walking in a deliberate, stiff, or awkward manner
- Acting in an unusually vigilant manner
- Having a blank facial expression, or appearing extremely focused or in a trance
- Exhibiting unusually calm and detached behavior

Letters or packages that contain a bomb or a chemical, biological, or radiological (CBR) threat may have one or more of the following characteristics. Handle them with great care. Don't shake, bump, smell, or open them. Put the letter or package down carefully and leave the area. Do not open windows. Call **911** from a landline phone if one is available outside the area. Otherwise it is OK to use a cell phone or pager. Wash your hands thoroughly with soap and water if you touched the letter or package.

- Are unexpected or from someone you don't know
- Are addressed to someone now longer at your address
- Have no return address or one that does not appear legitimate
- Are bulky, lumpy, or lopsided in appearance
- Have wires or other unusual contents that are protruding or can be felt through the envelope or wrapping
- Are sealed with excessive amounts of tape or string
- Have restrictive markings such as "Personal" or "Confidential"
- Have excessive postage
- Emit a strange odor
- Are mailed from a foreign country
- Do not have a named addressee, e.g., are addressed to a title only
- Have incorrect title or misspelled words in the address
- Poor handwriting
- Have oily stains, discolorations, or crystallization on the wrapper

For additional information see the U.S. Postal Inspection Service *Guide to Mail Center Security* at <http://about.usps.com/publications/pub166.pdf>.

If a suspicious object is found outside, get away from it after reporting it. 300 yards is a minimum distance. Then take cover for protection against bomb fragments. Get on the ground if no cover is available. Maintain distance and cover, or leave the area after an explosion. Be alert and cautious in reentering the area to help victims. There may be another device nearby.

Non-Emergencies. Call SDPD at (619) 531-2000 or (858) 484-3154

Non-emergencies are crimes and suspicious activities are ones in which: (a) there is no serious personal injury, property damage, or property loss; (b) the suspect has left the scene or is not likely to return; and (c) an immediate response is not needed. Because the waiting times to talk to a dispatcher are long during the day, the best times to call are before 8:00 a.m. and after 8:00 p.m.

The following are considered non-emergencies for reporting purposes.

- Persons or activities that do not appear to belong in the workplace, neighborhood, business establishment, or near a key facility or event because of their demeanor, behavior, language, dress, activity, etc.
- Multiple sighting of the same suspicious persons, vehicles, or activities at the same location
- Rental of storage units for suspicious items or activities
- Deliveries of chemicals directly to self-storage units
- Unusual deliveries of chemicals to residences or rural addresses
- Street people not previously seen in the area, i.e., panhandlers, shoe shiners, food or flower vendors, newsagents, street sweepers, etc.

Persons doing the following:

- Sitting in a parked vehicle for an extended period of time
- Loitering in public places, e.g., bus stops and train stations
- Loitering near or wandering around a possible target
- Carrying on long conversations on pay or cellular phones near a possible target
- Wearing military or other uniforms that don't appear to belong in them
- Observing security measures or personnel, entry points, access controls, and perimeter barriers such as fences or walls, at a possible target
- Testing or probing security measures, e.g., by driving by a sensitive area, attempting to enter a sensitive area, inquiring about security measures, attempting to smuggle contraband through check points, asking for directions, claiming to be lost, etc.
- Attempting to enter a key facility without proper ID, prior notification and approval, etc.
- Being in a key facility without required visible ID
- Staring or quickly looking away from personnel or vehicles entering or leaving a key facility or parking area
- Carrying heavy bags or backpacks near a possible target
- Setting down bags or backpacks near a possible target and then walking away
- Behaving as if they may be planning a terrorist act, e.g., by mapping routes, timing traffic lights or traffic flow, playing out scenarios, monitoring key facilities or events, etc.
- Observing activities and movements of police personnel, e.g., in and out of a police station.
- Possessing or distributing literature that promotes jihad, racist activities, or terrorist/extremist agendas.
- Seeking donations for obscure charities. You can check on whether a charity is registered as a nonprofit with the IRS at www.irs.gov/app/pub-78.

Vehicles that:

- Are parked near a key facility for an unusual period of time
- Are commonly used for deliveries, e.g., trucks, vans, or U-Hauls, that are parked in locations not usually used for deliveries without prior authorization
- Are out of place in the environment, e.g., a tractor-trailer parked in a residential neighborhood, and may have out-of-state or temporary plates
- Are abandoned
- Are overloaded or sagging (rear-weighted)
- Are leaking a fluid
- Have odor or gasoline, propane, acids, or chemicals
- Have been modified to handle heavier than normal loads, additional storage space, or increased fuel capacity
- Have excessively darkened or tinted windows, or temporary window coverings to prevent viewing of the vehicle's interior
- Show signs of theft, e.g., damaged locks, missing windows, etc.
- Have license plates removed or altered
- Bear a temporary commercial placard affixed with tape or magnets, or a permanent placard that is unusual, unrecognizable, or has misspelled words
- Contain batteries, wiring, timers, other power supply or switching components, unmarked packages or unusual items such as PVC pipe, magnets, compressed gas cylinders, fire extinguishers, etc. in the passenger compartment
- Have large containers on seats or cargo space (bags, boxes, barrels, tanks)
- Have cargo concealed under a tarp or blanket
- Contain blueprints, maps, sketching materials, or surveillance equipment, e.g., binoculars, video cameras, high-magnification lenses, etc. in the passenger compartment

Other Indicators of Terrorist Activities

Some examples of suspicious behaviors, activities to report, and other things you should do to help prevent terrorism can be found in the iWATCH section of the Los Angeles Police Department's website at

www.lapdonline.org/iwatchla/content_basic_view/42535. There you can learn about potential indicators of terrorist activities in the following areas: bulk fuel distributors, construction sites, dive/boat stores, farm supply stores, financial institutions, general aviation airports, hobby shops, home improvement and large retail stores, hotels and motels, peroxide-based explosives, rental cars, rental properties, rental trucks, shopping malls and centers, and storage facilities.

To suggest what people should look for, the SDPD has published the following eight indicators of terrorist activities. Persons seen or suspected of doing the following should be reported by calling **911**.

- 1. Surveillance.** Terrorists may conduct surveillance to determine a target's strengths and weaknesses. Be aware of someone who appears to be monitoring security personnel or equipment, or gauging emergency response time. Suspicious activities could include using vision enhancing devices, acquiring floor plans or blueprints, and showing interest in security and access to facilities.
- 2. Elicitation.** A terrorist may try to gain information about the operations and security of a potential target, possibly an important place such as a power plant, stadium, or school. It could be gathered many ways by phone, email, in person, or even by gaining employment at the location.
- 3. Testing Security.** Someone may use different methods to test security, such as trespassing into a restricted area or leaving a bag unattended in a public place to see how long it takes for people or security to respond.
- 4. Funding.** Terrorists need to raise money for their operations and spend it in a way that doesn't draw attention. This could be done many ways through crimes such as drugs and counterfeit merchandise sales, burglary, or even funneling money from legitimate businesses or non-profit organizations. Be aware of unusually large transactions paid with cash or gift cards, or someone soliciting a donation for a charity you've never heard of.
- 5. Acquiring Supplies.** To conduct an attack, terrorists may need a variety of supplies, such as weapons, transportation, and communication systems. Suspicious activities could include a vehicle left in an unusual place; stockpiling fertilizers, weapons, even one-time use cell phones; acquiring or stealing uniforms; and forging personal identification or passports.
- 6. Impersonation.** Terrorists may impersonate law enforcement officers, firefighters, EMS or paramedic personnel, mail carriers, or company employees to gain information. Someone who seems suspicious in what they say or do on the job could be a red flag.
- 7. Rehearsal.** Terrorists often rehearse a planned attack, possibly several times, to make sure their operation runs smoothly. This may include measuring response time by emergency responders, and possibly using police radios.
- 8. Deployment.** This is when terrorists are putting their plans into place, getting into position, moving equipment and supplies, and launching an attack.

Another terrorist activity is domestic radicalization to violence. Canadian experts involved in national security say the following traits indicate that someone is becoming radicalized. Every jihadist who has come to the attention of authorities there has exhibited several, if not all, of these traits. People with these traits should be reported to the SDPD by calling its non-emergency number, **(619) 531-2000** or **(858) 484-3154**.

- They abruptly abandon friends and family members.
- In the increasingly rare occasions where they do see their family, they berate them for their supposedly impious behavior. This might include accusing their father of being an infidel for consuming alcohol or calling their sister a slut for not wearing the proper headwear.
- They stop participating in activities that used to occupy a lot of their time, such as sports or community associations.
- They believe they have found the true path to religious enlightenment, usually in the form of radical Sunnism, and anyone who doesn't follow it is of less worth.
- They often exhibit growing hatred and intolerance toward others who don't adhere to their beliefs. This includes rejecting fellow Muslims of different sects, as well as imams who repudiate violence.
- They refuse to engage with or debate ideas that counter their own.
- They turn their back on their life as it was before radicalization.
- Surfing of pornography and violent jihadi/anti-government websites takes up increasingly large chunks of their day.
- They develop obsessive patterns of behavior and pine for martyrdom and the apocalypse.

With growing violent extremist activities overseas, it is also important to report people who are being recruited to go overseas, as indicated by the following behavior, or have returned from fighting overseas.

- Show new interest in regional conflicts
- Express support for violent extremist organizations
- Spend more time on the Internet watching violent extremist videos and frequenting websites, forums, or chat rooms with violent extremist group propaganda
- Communicate with persons associated with violent extremist organizations in person or on social media
- Change appearance
- Withdraw from community, family, and friends
- Learn to use weapons
- Start to save money for travel overseas
- Make suspicious travel patterns, e.g., buying one-way plane tickets

SDPD SECURITY SURVEY CHECKLIST FOR RELIGIOUS INSTITUTIONS

Date _____ Time _____
Institution _____ Phone (____) _____
Address _____
Institution Contact _____ E-mail address _____
Survey by _____ Phone (____) _____

Survey instructions: Put an X next to the number of each item that does not exist, and write an explanation on another page.

I. OUTSIDE

a. Fencing and Gates

1. At least 6 ft high
2. Open (chain-link or wrought-iron) fencing on property lines, or around or between buildings
3. Bottom of chain-link fencing secured with tension wire or galvanized pipe, or anchored to the ground
4. Horizontal bars on wrought-iron fencing located only at the top and bottom on inside of fence.
5. No holes in or under the fence
6. Shielded- or hidden-shackle padlocks on pedestrian gates that aren't emergency exits
7. Pedestrian and vehicle gates locked when institution is closed. Pedestrian gates that are emergency exits should open on the inside with a push or press bar and have shields that prevent the bar or latch from being depressed by simple devices, e.g., a knife blade or coat hanger.
8. Pedestrian and vehicle gates at main entrance can be open when the institution is open. Signs identify them as entrance for visitors.
9. Keypad or lockbox with fob or card for SDPD access at main pedestrian gate

b. Landscaping

1. Shrubs and hedges trimmed to less than 3 ft
2. Tree canopies trimmed to at least 8 ft
3. Higher bushes or trees with lower canopies OK next to a blank wall or the side of a building.
4. Thorny (defensive) plants in front of ground-level windows and other restricted-access areas
5. No hiding places behind bushes next to buildings or walkways
6. No views into or within the property blocked by trees or bushes
7. No loose rocks or other materials
8. Bushes next to building walls should be trimmed to leave a clear space of at least 12 inches between them and the wall so any objects left next to the wall can be seen in a walk-around inspection of the building.
9. Trees planted away from light poles and fixtures so they do not block any light, and from cameras so they do not block their fields of view.

c. Signs

1. Map and directory at main entrance shows names and locations of buildings, building numbers, room numbers in each building, etc.
2. Building names and numbers, and room numbers on buildings. Building numbers should be highly visible and not obstructed by trees. They should be at least 24 inches high.
3. Building numbers on roofs. For high contrast, numbers should be black on a white background. They should be at least 36 inches high so they can be seen from a helicopter at an altitude of 1000 ft.
4. Staff and other designated parking areas or spaces in lots
5. Directions to admin office, buildings, outside activity areas, emergency call boxes, etc.
6. Directing visitors to register in the admin office
7. Prohibitions on trespassing, loitering, public parking, skateboarding, etc. with California and San Diego Municipal Code sections cited
8. Staff-only and other restricted-access areas

d. Parking

1. Fenced and gated
2. Designated staff parking
3. Parking stickers for staff member's vehicles
4. School drop-off, waiting, and pick-up areas in view of main entrance
5. Parking spaces aligned with visual sightlines from buildings

e. Exterior Lighting

1. High-intensity and uniform on walkways, entrances, exits, parking lots, and other areas used after dark
2. No burnt-out bulbs or broken fixtures
3. Vandal-proof fixtures, e.g., wire-glass
4. No lights where people shouldn't go at night
5. Motion detectors control lighting around buildings and in areas not used at night
6. Not blocked by trees or bushes

f. Activity Areas

1. Designated uses for all areas on the property
2. Seating areas separated from walkways
3. No hiding or entrapment spots along walkways

g. Bike Racks and Lockers

1. Located in areas of good visibility and high foot traffic, or where use can be supervised
2. Separated from vehicle parking lot
3. Well-lighted for use after dark

h. Dumpster Enclosure

1. Located away from the buildings
2. Locks on doors
3. Locked lids on dumpsters
4. Located against walls or fences with no hiding spaces behind

i. Conditions and Protection

1. No graffiti, trash, litter, junk, debris, etc.
2. Anti-graffiti paint or coatings on walls, signs, light poles, etc.
3. No skateboard damage on benches, low walls, etc.
4. Skateboard prevention devices, e.g., small metal or plastic discs or strips on the edges of raised surfaces,
 1. and small metal discs or bolt heads on tops of railings
5. Tops and edges of seats and low walls shaped to prevent skateboarding
6. No gasoline, flammable chemicals, or other potential fire hazards
7. Art works designed to be vandal-resistant and easy to repair

II. INSIDE BUILDINGS

a. Admin Office

1. Located in a building at main entrance to the institution
2. Windows that provide unobstructed view of the walkway leading to the front door
3. Counter or desk in lobby with unobstructed view of the front door and adjacent stairways and corridors
4. Video intercom for admitting visitors when the front door is locked
5. Log for visitors and delivery/service people to sign in and be issued a visitor badge
6. Police, fire, and other emergency numbers kept by phone. **911** for all emergencies and **(619) 531-2000** or **(858) 484-3154** to the SDPD for non-emergencies. And the name and phone number of the local SDPD Division CRO for other matters. The latter should be updated periodically because officer assignments change.
7. Panic alarm button
8. Monitor and controls for surveillance cameras.
9. Display for status of alarmed doors and windows

10. Command and communications (C2) center for emergencies. Receives calls from emergency call boxes
11. Files, records, etc. kept in locked, fireproof containers or vaults
12. Duplicates of all files, records and computer disks kept off campus
13. Annual update of insurance on buildings and contents

b. Doors

1. Two-way visibility in doors at building entrances, stairways, corridors, etc.
2. One-way visibility (inside to outside) or peepholes in doors to staff-only areas
3. Outside door hinges with non-removable pins
4. Deadbolt locks on exterior doors. Latch guards on doors with beveled latches.
5. Open with access cards or keys that cannot be duplicated
6. Access to offices, kitchen, electrical and mechanical rooms, storage rooms, etc. limited to institution staff
7. Rooms locked when not in use
8. Alarmed, self-locking emergency exits with sign FOR EMERGENCY USE ONLY.
9. No gaps between double doors, between single doors and their frames, and under doors that open on the inside with lever arms or press bars
10. Separate deadbolt locks on double doors with gaps between them, single doors with gaps between them and their frames, and doors that open in the inside with lever arms or press bars with gaps under them

c. Exterior Windows

1. Strong glass, i.e., laminated, tempered, or wired to prevent easy break-ins.
2. Safety and security film attached to the inside of standard glass windows, which shatter easily when hit with blast wave. Flying glass then becomes lethal to people inside.
3. Not obstructed by signs, displays, plants, etc. for good views of outside activity areas
4. Shutters, shades, or blinds for use in an emergency to prevent a person from seeing into the room

d. Interior Windows

1. Safety and security film attached to the inside of standard glass windows, which shatter easily when hit with blast wave. Flying glass then becomes lethal to people inside.
2. Shutters, shades, or blinds for use in an emergency to prevent a person from seeing into the room

e. Interior Corridors

1. Wide enough for smooth traffic flow
2. No obstructions, e.g., display cases, fountains, etc.
3. Well-lighted with light-colored walls
4. Mirrors to see around corners and into alcoves

f. Exterior Walkways

1. Wide enough for smooth traffic flow
2. No obstructions, e.g., benches, trash containers, vending machines, etc.
3. No hiding or loitering places in doorways
4. Open handrails on upper-level walkways
5. Well-lighted
6. Canopies supported by slim columns
7. Mirrors to see around corners and into alcoves

g. Stairs

1. Strong glass windows in doors to interior stairs
2. Exterior stairs visible to surrounding area, i.e., not out-of-sight behind buildings
3. Open exterior stairs with open handrails, i.e., not enclosed by solid walls

h. Elevators

1. Use limited to authorized individuals, e.g., institution staff, handicapped persons, etc.
2. Central location in buildings
3. Doors visible from interior corridors

i. Staff Offices

1. Doors and interior walls have windows to interior corridors or common reception area
2. Exterior windows have views of outside activities

j. Classrooms

1. Doors should be lockable from inside the room, but must normally be openable from the inside by children without the use of any key or special knowledge or effort.
2. Shutters on windows in doors for use in an emergency to prevent a person from seeing into the room
3. Exterior windows should have strong glass, i.e., laminated, tempered, or wired, to prevent easy break-ins.
4. Standard glass windows should have a safety and security film attached on the inside because they shatter easily when hit with blast wave. Flying glass then becomes lethal to people inside.
5. Exterior windows should not have signs, displays, plants, etc. that would obstruct good views of outside activity areas. But they should have shutters, shades, or blinds for use in an emergency to prevent a person from seeing into the room.
6. Equipment for receiving and responding to emergency messages from admin C2 center
7. Phone with direct outside line
8. Silent alarm to admin office

k. Restrooms

1. Located on main corridors or walkways near high-activity areas, not behind buildings or in separate corridors
2. Single-door entrances
3. Open tops and bottoms of toilet-stall partitions and doors
4. Vandal-proof facilities

l. Storage Rooms

1. Locked and alarmed doors
2. Interior location with no exterior windows and doors

m. Roof

1. Not accessible by climbing trees, building-mounted ladders, walls, support columns, etc.
2. Unbreakable skylights
3. Locked enclosures for air conditioning, cooling towers, etc.
4. Painted building number. For high contrast it should be black on a white background. It should be at least 36 inches high so they can be seen from a helicopter at an altitude of 1000 ft.

III. SECURITY MEASURES

a. Security Guards

1. On duty when institution is open
2. Random patrol when institution is closed

b. Burglar Alarm System

1. Exterior doors and windows
2. Motion detectors in areas and rooms with high-value items
3. Glass-break detectors

c. Fire Alarm and Suppression System

1. Smoke and fire alarms connected to a central monitoring station or directly to the fire department
2. Batteries tested at least once a month and replaced at least once a year
3. Fire suppression sprinkler system
4. Fire extinguishers at designed locations
5. Hoses at exterior faucets

d. Access Controls

1. Keypads or card readers on all doors
2. Access limited on “need-to-enter” basis
3. Roll- or drop-down security screens on corridors that lead from the reception desk or counter into the building

e. Cameras

1. Located in property and building entrances, parking lots, interior corridors, exterior walkways, etc.
2. Record high-quality, digital imagery continually, when motion is detected, at specified times, or on an alarm. CCTV or IP cameras can be used for this.
3. Programmable IP cameras with video-analytics software, so-called “smart” cameras, are needed to record when specific alert conditions occur.
4. Monitored in admin office during office hours
5. Monitored at security (burglar alarm) company office after hours

f. Communications

1. Emergency call boxes in main activity areas
2. PA system for entire facility
3. Two-way communications with staff
4. Rapid emergency response communication system that will contact law enforcement and alert building occupants to take precautions immediately.

g. Property Identification and Security

1. ID markings on all valuable removable items
2. Photos or videotapes of all valuables
3. Inventory of all furniture and equipment with model and serial numbers
4. Computers and other valuable removable items secured to tables or other fixtures

h. Cash and Key Control

1. Secure room for handling cash
2. Drop safe for storing cash
3. List of staff members with various keys
4. Means of collecting keys from departing staff members

i. Institution Staff Members

1. Wear photo ID badges
2. Greet and offer to help visitors and strangers. Escort visitors without badges to the admin office to register and get a badge.
3. Report non-emergency crimes, suspicious activities, rumors, trespassers, etc. to admin office. Call 911 to report emergencies
4. Check that doors and windows are locked, alarms are set, night lights are on, etc. at the end of the day
5. Trained in security procedures and responses to various emergencies
6. Participate in periodic drills and exercises for various emergencies

j. Visitor Control

1. Designated Parking
2. Signs directing visitors to admin office
3. Visitor badges issued at and returned to the admin office
4. Verify IDs of delivery/service people and contractors

k. Emergency Procedures

1. Emergency procedures manual. In addition to procedures for dealing with fires, earthquakes, and medical emergencies, the manual should include procedures for dealing with the following crime emergencies: telephone bomb threat; telephone chemical or biological threat; suspicious envelopes, packages, and deliveries; armed intruder; armed trespasser; active shooter, vandalism in progress; robberies; burglary in

progress; suspicious persons, objects, activities, and vehicles; child abduction; bullying; etc. Review and update procedures periodically.

2. Alternate C2 center
3. Evacuation plans posted in each room and activity area
4. Designated safe and secure areas on the grounds
5. Lockdown for rooms and buildings
6. Emergency evacuation and other drills
7. Dealing with armed intruders and active shooters. The DHS paper entitled *Active Shooter How to Respond* provides a great deal of useful information on how to respond when an active shooter is in your vicinity, what to do when law enforcement arrives, how to train your staff for an active shooter situation, etc. It can be downloaded from the DHS website at www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf.

l. Working with the SDPD

1. Provide it with campus site plan, floor plans and elevations of all buildings, and descriptions of the activities in each room
2. Allow it to take pictures on the campus for use in training officers to respond to emergencies
3. Have it review emergency procedures
4. Invite to participate in security exercises
5. Give it a Letter of Agency to authorize it to act as your agent and enter your property for purposes of enforcing laws against any person(s) found on the property without your consent or without lawful purpose.
6. Post its NO TRESPASSING signs stating that a Letter of Agency has been filed.

m. Hardening

1. Bollards at entrances to prevent vehicles from driving in
2. Films or protective shields on windows to prevent bombs from being thrown through
3. Films on windows to prevent fragmenting and flying glass from outside blasts
4. Drapes on windows to catch flying glass fragments from outside blasts
5. Blast-resistant walls between the buildings and adjoining streets and parking lots