Keeping Your Jewish Institution Safe

Online Edition

ADL Anti-Defamation League®

ANTI-DEFAMATION LEAGUE

Copies of this publication are in the
Rita and Leo Greenland Human Relations Library and Research Center

Web site: **www.adl.org**

ADL is pleased to make this special pre-publication of *Keeping Your Jewish Institution Safe* available. Due to the need to expedite the printing of this publication some errors or omissions may have occurred.

Keeping Your Jewish Institution Safe:

Special Edition

Forthcoming Sections: (Check our Web site for updates**)**

Security in Jewish Communal Life: Building Consensus, Training and Preparedness, and Computer and Data Security.

Using This Manual

The following security awareness manual is designed to help you begin the process of thinking about security for your institution. However, it is by no means an exhaustive treatment on the subject of security (no such document exists). Moreover, it is not a security plan for your institution. Rather, it is a series of *security considerations*.

What distinguishes security considerations from a list of security recommendations? The set of facts and circumstances unique to every institution will dictate what you choose to implement. You know your institution, you know its finances, and you know what security measures constituents will accept (and what leadership can help constituents learn to accept). Thus, when we offer suggestions or lists, you must evaluate those thoughts in light of your institution.

> You must bear in mind that not every item on a list is applicable to your institution and that not everything applicable to your institution is on these lists.

One way to use this manual is as a starting point for a conversation with you, selected members of your staff, lay leadership and a security professional who can assess your institution first hand.

All this said, we believe this manual will be helpful as you begin the process of developing a plan for your institution.

> **Remember: Your ADL Regional Office is a resource available to you. Please see the list of Regional Offices at the back of this document.**

Introduction: Security Planning

Creating secure Jewish communal institutions must include the design of a security plan. A sound security plan will leave an institution better able to thwart and, if necessary, recover from, a security breach. Remember: the best way to protect your institution is to prepare for and prevent an incident's occurrence in the first place.

A sound security plan in a Jewish communal institution is often as much a management issue as it is a technological one. It involves motivating and educating all staff, leaders and community members to understand the need for security and to create and implement a coherent security plan. In general:

Professionals and leadership should assess the risks and realities of the institution to develop a security plan, seeking professional guidance if necessary. Of course, not all institutions run the same risk, but *all* run some risk. Most critically, leaders must make sure that security is part of an institution's culture (*see* forthcoming chapter on "Security in Jewish Communal Life: Building Consensus"). At the very least, input on security should be sought from all staff (not only is their "buy-in" essential for a smoothly running plan, but they are also important "eyes and ears"). When planning or participating in events, everyone – ranging from the Board President to the custodial staff – must *think securit*y.

Community members have an important role in ensuring the safety of their communal institutions. Leadership can help them understand their role in the plan. Community members should:

- be watchful, be ready and be willing to report suspicious activity;
- know their building -- report anything that is out-of-place or missing;
- actively cooperate with security directions, check-in procedures and ticket policies;

- help create a culture that is both secure and welcoming; care about security -- and let people know that they care, and
- support the board and professionals as they make the decision to create and implement an effective security plan.

Creating a Security Plan

While no guide can provide you with a "one-size-fits-all" security plan, there are certain basic considerations that all security planners must take into account. This guide will help you understand and apply those elements. ADL continually publishes new information on security and invites you to visit www.adl.org/security for new materials and updates.

Notably, creating a plan, and even installing hardware and/or hiring additional staff, are not the end of the process. Once the plan is written, make sure that all leaders, employees and constituents know it, practice it, review it and implement it. Regular training on, and review of, your security plan are critical parts of an institution's security.

Creating a secure environment is a three-step process: *Assessment, Planning and Implementation.* **You may wish to consult with your local police and/or hire a professional security firm for assistance in this process.**

As you read through these preliminary considerations, remember that many of these topics are discussed in detail throughout this manual.

- **Assess**:
  - **Potential Threats**: Identify the potential threats specific to your institution
    - What does the news tell you about the current national and international climate?

- What do the local police tell you about the local climate?
- What does your ADL Regional Office say about extremist and anti-Semitic activity in your area?
- Is there something about your building or your staff that would attract a terrorist attack, such as high-profile programs, high-profile members or an extremely visible building?
- Are you at risk from collateral damage from an attack on a high-risk neighbor (e.g., political offices, controversial corporate offices, family planning clinics)?
- Are you at risk from employees or other "insiders"?
- Is it too easy to find your institution? The question of directional signs on public streets is one only your institution can answer. ADL takes no position on this difficult question.

- **Identify Targets for Protection.** Identify what you need to protect (e.g., people, property and data) and what makes those things vulnerable. There are different strategies for protecting children, adults, property and data and your planning must account for these strategies. Note also that sometimes these things are related: the theft of a computer that contains membership lists and payment information can do great damage to an institution's reputation and the members' safety.

- **Relationships with Law Enforcement.** This manual will stress in many places: developing a working relationship with your local law enforcement agencies is very important. At the very least, your local police department may have a crime prevention officer who will do an on-sight security inspection and review your plan. Not only will this provide useful information, but it will help build a relationship with your local law enforcement.

- **Plan:**
  - **Risk Reduction.** Identify the most appropriate measures to reduce your risk, recognizing that you can never completely eliminate all risk. Your most appropriate initial steps may be as simple as replacing/re-keying the locks to gain control over who has keys to the building.

  - **Command, Control and Communications**. In any emergency event, firm lines of command, control and communications are essential.
    - It is vital that a decision maker be identified, that this person have the authority to act, and that the decisions can be effectively communicated to those who need to know them.
    - It is also important to recognize that a designated decision maker may be unavailable during an emergency (he/she may be out sick or on vacation or even at lunch or away from the office for a meeting). Thus, it is important to be able to quickly ascertain who is in charge at any given point. Consider having a list of "succession" in the event of an absence, even a temporary one.

  - **Explosives Planning.** Planning should include creating and maintaining a bomb search plan and emergency evacuation plan.

    - This is an important time to contact and include your local bomb squad. They will help you understand what steps you are responsible for implementing in a bomb emergency (searching) and when they will respond (many bomb squads will not come to a site until a suspicious item has been discovered). As many bomb squads do not allow individual organizations to contact them, communicating with your bomb squad may require that your request go through the local police department. This is yet another reason to develop a relationship with your local police department. Your ADL Regional Office can help in this regard.

- Your evacuation plan should include ways to notify and, if necessary, evacuate everyone in your facility in an emergency. Designate a meeting point to ensure that everyone is safe.

- **Varied Use Plans.** You should create plans that deal with the varied uses of your buildings. School days, high traffic events (such as the High Holidays) and days when the facility is not used all create different security circumstances.

- **Business Recovery.** Planning should include business recovery strategy and a review of insurance. Such business recovery plans may include off-site data storage (including vendor and membership lists) and plans for emergency corporate governance, etc.

- **Available Resources.** Work with security specialists, the police, other emergency services and your Anti-Defamation League Regional Office.

❖ **Implement**

- **Accountability: The Security Manager.** Designate a member of your staff to serve as security manager, accountable for implementing, reviewing and constantly updating the plan. Make sure everyone is trained to implement the plan -- especially those who will be on the front lines of using the plan and those who know your building best: your maintenance personnel.

  The security manager should be a member of the senior staff, yet he/she should have enough time to fulfill his/her security responsibilities, especially when he/she first assumes the position (for, as in most institutions, the security manager has no security experience and thus may have a significant learning curve and time commitment). This person is responsible for continued training and for updating the plan.

- **Training is critical**: Conduct communal and staff training, drills and role playing, and regular refresher exercises. Drills and role playing ensure that the plan is workable, up-to-date and fresh in people's minds.

- **Implementation of a plan**: Constantly reassess and update your plan.

- **Build relationships**: At every stage, work to build relationships with your local emergency services. Get to know local law enforcement, and get them to know you, *before* there is a problem. Invite local police officers to use your gym, to join you for an *oneg shabbat* or just to visit your building and get to know it.

Other thoughts about the planning process:

No one plan works for everyone. However, depending on what is best for your institution, you may wish to consider the following. Remember, these topics are discussed in detail later in this manual.

- Ensure that entrances to your building are monitored; no one should enter your building unscreened. There are many ways to screen, including using ushers, volunteers, staff, etc. The installation of closed-circuit TV cameras, intercoms and door release systems can assist in this process. Your security plan should develop and implement policies to ensure that screening is ongoing.

- Minimize the number of open entrances to your facility (consistent with fire codes). A culture that promotes security consciousness allows staff and visitors to understand that minor inconveniences may translate into major security benefits.

- Have all emergency phone numbers readily available. While you should always try to use 911 first in an emergency, you should also have the local phone number

of your local emergency responders readily available. Have a cell phone to use to call emergency services from outside your facility (ensure that all local emergency numbers are pre-programmed into that phone). Note: *do not use a cell phone or walkie-talkies during a bomb-related emergency as any device using radio waves may cause a device to detonate.*

- Have a disposable camera available. This way, you can take pictures (when it is safe to do so) that may assist police if a suspicious individual or car is seen.

- Regularly inspect your building. You should be able to quickly ascertain if something is amiss and help law enforcement if there is a problem.

- Use the security devices you already have. This may sound like a truism, but ensure that security devices are turned on and are functioning, that outdoor lighting is working, that windows and fence lines are kept clear of bushes, and that access to your building is appropriately limited and consistent with fire codes.

- Think security. Each person is a "deputy" in the effort to maintain proper security. Good security practice flows down from top management. It is important for administrators to share security information with their staffs and with lay persons to increase the security consciousness of the entire organization. Security awareness should be built on a broad base which begins at home, continues on the street and public transportation and culminates with sound security planning and practices in the employees' work areas. The key point is to recognize unusual activity.

A word on . . .

Security committees. A security committee can help bring staff and leadership together to ensure that there is maximum "buy-in" to a security plan. Indeed, depending on the type of institution, professionals and leadership working

together can help ensure that the institution's wider constituency accept the plan and thus complies more readily with implemented changes –something that can mean the difference between effective solutions and failure. Moreover, leadership can work to reassure constituents, without revealing too much, that the institution takes security seriously. Thus, we suggest that security planning is a process that may be undertaken by a security committee.

Small and mid-size institutions. This manual was written with all size institutions - and all size budgets -in mind. Remember: many of the suggestions included in this manual are no-cost or relatively low-cost ideas (e.g., using ushers, re-keying locks for key control, etc).

Security "philosophy." Security is a long-term issue. It is not something that one can effectively address every time there is a new alert or increased sense of risk. Solutions implemented under such circumstances can be costly, less effective than solutions implemented as the result of careful planning. In other words, security is something to be addressed rationally and in a considered fashion, not reactively and out of fear.

Finally, a security expert can help you fully examine these issues, and create a plan to implement.

Physical Security

Important Note

While the suggestions offered in this chapter can be quite detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the suggestions given below as the starting point for discussions with a security professional who will be able to assess your institution's particular set of circumstances and make specific recommendations.[1]

Physical Security

Physical security starts with a rather simple basic premise: those who do not belong on your institution's property should be excluded from your institution. This may happen in three (often interrelated) ways:

1. When those who do not belong are identified, stopped and denied admission by a person.
2. When those who do not belong are denied admission by a physical device, such as by a locked door.
3. When those who do not belong are denied admission because they decide that your institution is too difficult to enter and thus they do not even try.

This section will consider the various methods of excluding those who do not belong:

1. Access Control
2. Key Control and Locks
3. Protective Devices/Alarms
4. Windows and Doors

---

[1] Given the specific information discussed in this chapter, it is important to again specifically mention that neither this guide nor this chapter is intended to provide comprehensive, institution-specific advice on security matters nor is it meant to replace the advice of a security professional. For comprehensive, institution-specific security advice, a security professional should be consulted. ADL specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of the use, nonuse or misuse of this information.

5. Fencing
6. Lighting
7. General Target Hardening

Access Control

Access Control means that, when your facility is open, no visitor, delivery, service person, or unknown individual is able to enter your facility without both being observed (directly or indirectly) and approved. Several techniques to accomplish that goal may include:

1. **Security desk**. A security desk should be set up in the main lobby of each building which has an open-access or open-door policy. A sign-in/out log book, supervised by an employee who validates identification *prior* to allowing visitors to proceed into the building, is highly advisable.

2. **Monitored entrances**. Ideally, an institution should have a single entrance only, monitored by a staff person and equipped with an intercom system for communicating with anyone who comes to the door. External barriers may also be considered. Simply, an open door policy does not mean that every door needs to be left open and unlocked.

3. **Checking credentials**. Before allowing a person to enter institution property, make certain his/her identification papers or other credentials (including membership cards) are valid. Police and most utility employees carry identification cards and other documents. It is critical to remember that one must question whether employees can tell the difference between valid and forged documentation or credentials. While it is true that police and most utility employees carry such identification it is questionable whether your staff can be expected to tell the difference between the real and the fake. It is very easy to purchase a uniform or equipment that enables an intruder to pretend that he/she

has legitimate reason to enter your facility. It is worth a few moments to contact the person's company or organization to determine the legitimacy of the person requesting admittance. Never be embarrassed to ask for more identification or to ask a person to wait until his/her identity may be checked. Any individual who becomes agitated or angry at such a request should be considered of questionable legitimacy.

4. **Visitors**. At no time should visitors be allowed to roam freely through your property unescorted or without being observed. That is especially true for individuals who expect to work on your most sensitive systems such as burglar alarms, fire alarms, communication systems, or computers. Special diligence should be applied to those individuals when they visit your institution. For larger institutions, certain areas should be considered off-limits to all but authorized personnel.

   Note: Some institutions specialize in open and free access, e.g., facilities with gymnasiums. Allowing visitors free access to your facility does not mean that they should be allowed to go anywhere (e.g., into restricted areas such as office spaces) or that they are given a sense that their actions are entirely unnoticed by the institution's personnel.

5. **Stay-behinds**. End-of-day locking procedures should include a visual examination of all areas of the institution to prevent "stay-behind" burglars.

6. **Photo Identification**. All employees should have identification cards. Such cards make identification of non-employees immediate, and questions of identity are easily settled by producing the cards. It is recommended that all employees be provided and wear photo identification cards. Such cards will not only enable individuals to immediately identify those who work in an institution but will psychologically help employees understand that they are part of their agency's

security apparatus. Photo identification should not be handed out without accompanying education about their care, the procedure to be followed if they are lost, as well as the manner in which employees should approach unknown individuals.

Using ID cards requires care. Cards should have clear pictures along with the employees' names. It is debatable whether the institution's name should be placed on the card. In any event, employees should be instructed that their card should be prominently worn while in the building and, for their own safety, kept from view when away from the building. There is no reason why any person on the street or in a train should be able to identify who you are and where you work. Lost cards should be reported immediately.

Key Control and Locks

- **Key Control**

  Knowing who has which keys to which locks at all times is a vitally important issue. Failure to maintain such control may defeat the entire purpose of creating a security system. Institutions often simply assume that no one leaving their service - either an employee or volunteer - will subsequently break into the system. A sound key-control policy is essential to a sound security program. There should be a central key control location where masters are kept and to which entry is strictly controlled by management. Other thoughts:

  1. **Registry**. A central key control registry should be established for all keys and combinations. Employees and leadership should be required to sign for keys when they are received and the return of keys should be an important part of ending service.
  2. **Issuance**. Supervisory approval should be required for the issuance of all keys and locks. Spare keys and locks should be kept in a centrally located

cabinet, locked under the supervision of a designated employee. Master keys should be issued to a very restricted number of employees and these should be checked at least twice each year.

3. **Re-keying**. When key control is lost, it may be worthwhile to have an institution's locks re-keyed.
4. **Combination Locks and Codes**. Where combination locks and coded locks are used, those combinations and codes should be changed *at least* every six months or when employees or leadership leave service. The combination should also be kept under strict control of management.
5. **Special Keys**. It is good policy to use locks with keys which cannot be duplicated on the outside without special key blanks.
6. **Key Card Readers**. Key card readers, while expensive, make key control and locking more effective and nearly automatic.

- **Locks**

  Locks are, of course, particularly important to security. We suggest consulting a professional locksmith. While the suggestions offered in this section are especially detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the suggestions given below as the starting point for discussions with a professional locksmith who will be able to assess your institution's particular set of circumstances and make specific recommendations

  Door locks should be chosen and installed to provide proper security for the location involved. Locks with single cylinders and interior thumb turns, installed on doors with glass panels, should be placed more than 36 inches away from the nearest glass panel. Dead-bolt locks are the most reliable and should seat at least an inch into the door frame or lock-bolt receiver. Padlocks should be of high-grade material designed to withstand abuse and tampering. **At all times, the door-locking system must meet the fire code to allow emergency exiting without impediment.**

Further Lock Considerations:

1. **Exterior Locks**. All exterior door lock cylinders should be protected with metal guard plates or armored rings to prevent cylinder removal. The guard plates should be secured with round-head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.

2. All exterior locks should conform to the following:
   a. Lock cylinders should be highly pick-resistant.
   b. Where possible, dead-bolt locks should have a minimum bolt extension of one full inch.
   c. Drop-bolt locks should be installed with the proper strike: wood frame, angle strike; metal frame, flat strike.
   d. All exterior door-lock cylinders should be protected with metal guard places or armored rings to prevent cylinder removal. The guard-plate should be secured with round head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.
   e. The jamb must also be sufficiently strong as a strong lock entering a weak jamb will fail.
   f. **At all times, the door-locking system must meet the fire code to allow emergency exiting without impediment.**

3. **Automatic Closers**. Doors that have air, hydraulic or spring returns should be periodically tested to ensure that doors return to their fully closed or locked position.

4. **Lock Management**. Your institution's security manager should be responsible for the following:
   a. Regularly inspect and report all defective and damaged locks; repair quickly.

b. Establish a chain of responsibility for all locks (doors, windows, etc); ensure locks which are to be locked are in fact locked and report all failures to do so.
c. See that keys are not left unattended.
d. Recommend installation of additional locks where necessary.
e. The locking key control program should be part of your periodic security audit.

5. Remember: locks are present not only on doors, but on windows, offices, filing cabinets and storage closets as well.

Protective Devices/Alarms

This is an area where professional advice is particularly needed. Begin by contacting your local law enforcement agency and request help from the crime prevention, crime resistance, or burglary prevention officers who are specially trained and can offer expert guidance. Keep in mind that an officer is not selling a product or system but is there to help you.

- **Protective Devices**

Protective devices -- intrusion detectors, fire detection, alarm systems and cameras slaved to a Closed-Circuit TV (CCTV) system -- can be an important (and sometimes costly part) of an institution's security. CCTV coverage may also be useful as such systems permit surveillance of exterior exits and interior halls by one trained security officer at a master console. However, even the most sophisticated and costly devices are limited by the human factors involved. The best CCTV system will not be effective if they are not properly monitored or if those tasked with monitoring the cameras are overworked, poorly trained, tired or distracted. Additionally, most institutions are unlikely to have the resources for continual monitoring. An alternative is a videotape system, but here, too, the best video surveillance system will fail when not properly used, e.g., when no one is assigned the job of checking, reviewing and changing the tapes.

A few additional thoughts on surveillance cameras:

1. Surveillance cameras should be placed at the entrance points to your institution to act as a deterrent to potential intruders. Cameras can document criminal acts that may occur on your property. This documentation can be used to identify and prosecute perpetrators. Although expensive to purchase initially, these cameras generally prove to be economical when compared to potential loss.
2. Use a wide angle lenses to survey entrances.
3. Use cameras that employ infrared illumination to enhance night-time video.
4. Couple the camera with a time-lapse recorder for permanent recording.
5. Make sure your camera has a time/date recording capability.
6. Compare the cost of color versus black and white.
7. Save video film for a minimum of 72 hours.
8. Replace video film at least every six months.

- **Alarms**

This is another area where professional guidance is strongly recommended. Alarm systems are designed to protect your institution from intrusion. The installation of an alarm system can materially benefit the security of most institutions. The sophistication and coverage provided vary widely from system to system.[2]

The size, location, and type of institution will help determine the type of system required. Special features such as emergency panic buttons and robbery signal circuits may be considered.

---

[2] Alarm systems are made up of three components: (1) a sensor, which detects an intruder, (2) a control, which receives information from the sensor and (3) an enunciator, visibly or audibly alerting someone of the intrusion.

Motion detectors or automatic sensors that respond to sound or movement are excellent protective devices used alone or in conjunction with your institution's lighting system. These detectors and sensors are economical and they can be used inside or outside of your setting.

Because there are many alarm systems on the market you should research each system and select the one that best suits your needs.

Two effective, inexpensive solutions are alarms that use magnetic contacts and trip wires. Alarms with motion, sound, or light detectors are more expensive but are also generally more dependable. Whatever the amount of money you choose to invest in a dependable alarm system is generally less than the amount of damage that might be caused to your institution by an intruder.

When installing an alarm system, consider the following:

1. Make sure all alarm systems have emergency backup power sources.
2. Conceal the alarm control box and limit access to it.
3. Choose the system that best fits the need of your establishment.
4. Every system should have an electronic circuit delay of 30 seconds.
5. Ensure that the alarm can be heard throughout the property and have the alarm system monitored by a central alarm monitoring company.
6. Make sure all wiring components and sirens are protected from tampering.
7. Make sure the alarm comes with a "test" option. Testing the system regularly is a vital component of maintaining the effectiveness of your alarm.
8. Place alarm warning stickers in windows and/or entrances and exits.
9. Ensure that your alarm system comports with the legal requirements of your city or town (e.g., some prohibit directly dialing to police).
10. False alarms are a chronic problem. Staff and leadership should fully understand how to use the equipment and how your monitoring company will handle any and all alarms.

11. Consider adding "panic buttons" to your alarm system. Such buttons allow you to trigger the alarm from locations other than the alarm's main panel. You may wish to place these in key offices that are used during off hours, and in locations where intruders may first be confronted, such as in reception areas.

Windows and Doors

- **Doors**

All external doors, main building doors, and lobby doors leading to common halls should conform to the following guidelines:

1. Solid core, wood or metal.
2. Glass door panels or side panels should be reinforced either with metal or some form of steel mesh. Barring that, they should be replaced with a glass that does not shatter easily.
3. Where there is an alarm system, “glass breaker” sensors that detect glass breakage should be installed close to glass doors or windows.
4. Door frames should be sturdy and appropriate for the type of door. Weak frames should be replaced or rebuilt.
5. Exterior door locks should conform to the guidelines found in the section on locks.
6. Interior or office doors should be equipped with heavy duty, mortised latch sets that have dead-bolt capability. Rim-mounted, dead-bolt or drop-bolt locks can be installed to increase security of important offices or rooms.
7. Doors that have external or exposed hinges may be vulnerable to pin removal. The hinge pin should be made nonremovable by spot welding or other means or the hinges should be pinned to prevent separation.
8. Doors to utility closets should be equipped with dead bolts and kept locked at all times. Such closets, if unsecured, can become hiding places for “stay-behind” criminals or for explosive devices.

9. All exterior doors which do not have glass vision panels should be equipped with wide angle viewers (peep holes).
10. Interior doors should have two-way visibility at stairways, corridors, etc. There should be a clear view of room interiors from the doorway.
11. Access to offices, kitchens, electrical and mechanical rooms, and storage rooms must be substantially limited to appropriate staff and be locked when not in use.
12. Fire doors must conform to all local fire and building codes and should have an underwriters laboratory rating:
    A. Fire doors should be secured with approved latching or locking hardware, such as a panic bar with a spring latch or safety lock
    B. If a fire door has a solid core, the interior material must be fire resistant
    C. An adjustable spring or air return will ensure that the door is always closed
    D. As with all doors, sensor devices connecting to a sound device or system will announce their opening
    E. All doors or gates not observed either directly or remotely should be kept secured.
    F. Consider the possibility of placing height marks next to exit doors to help employees estimate height of suspicious persons.

- **Windows**

Windows should provide light, ventilation and visibility, but not easy access. Glass bricks can be used to seal a window, allowing a continued light source while providing increased security, although visibility and ventilation will be diminished. Gates and expanded steel screening, while often unattractive, will provide a high degree of security. Local building codes and fire safety regulations should be consulted prior to all such installations to avoid costly violations. Also, note that

skylights, ventilators and large door transoms can provide easy access to intruders unless properly protected. If permanent sealing is not possible, steel bars or screens of expanded metal may be required (if permitted by fire codes).

A Critical Note on Glass

Flying glass can be as dangerous in an explosion as the actual explosion itself. Consider replacing traditional glass with safety or shatter-resistant glass or using a clear protective film to secure the glass to the frame.

Fencing

Fences make an intruder's entry more difficult and give the appearance of a more secure institution. The following thoughts need to be prefaced with an important warning applicable to all sections of this manual: take note of all local building and zoning codes regarding fences prior to planning or contracting.

Some thoughts to bear in mind:

1. Consider open ornamental fences -- in preference to walls -- as they do not block visibility, are less susceptible to graffiti and may be more difficult to climb.
2. Fences should be at least six feet high. Therefore, an institution should take advantage of any small incline or hillock along which to build the fencing.
3. Fences should also be designed so that a person cannot reach in with their hand or a wire to open the fence gate from the outside.
4. If a panic bar is required on the inside of a fence gate, a solid metal or plastic shield should be used to prevent a person on the outside from opening the gate.
5. It is important that whatever physical barrier one erects should be in concert with the aesthetics of the neighborhood or environment. <u>It is</u>

unwise to alienate neighbors who may serve as part of a neighborhood watch and provide additional "eyes and ears" as part of your overall security program.

6. Walls should be constructed where there is a need for privacy and/or noise control.
7. Fence lines should be kept free of trash and debris. Clear away trees and vines that might aid a climber. Weeds and shrubs along fence lines, sides of buildings, or near entrance points could hide criminal activities. Keep shrubs low - under 36 inches - or clear them away completely. Cut back vines attached to buildings in order to prevent determined intruders from gaining access to upper windows or unprotected roof doors.
8. **Note:** it is impossible to erect an impenetrable physical barrier that is unprotected by personnel. Even when protected by personnel, human beings grow fatigued, inattentive, bored, or simply make mistakes.

Protective Lighting

The value of adequate lighting as a deterrent to crime cannot be overemphasized. Adequate lighting is a cost-effective line of defense in preventing crime.

1. Lighting, both inside and outside, is most helpful and can be accomplished without becoming overly intrusive to neighbors.
2. All entrances should be well lit. Fences should also be illuminated.
3. For outside lighting, the rule of thumb is to create light equal to that of full daylight.
4. The light should be directed downward away from the building or area to be protected and away from any security personnel you might have patrolling the facility.
5. Where fencing is used, the lighting should be inside and above the fencing to illuminate as much of the fence as possible.

6. Lighting must be consistent to reduce contrast between shadows and illuminated areas. It should be uniform on walkways, entrances, exits, and especially in parking areas.
7. Perimeter lights should be installed so the cones of illumination overlap, eliminating areas of total darkness if any one fails to light.
8. The fixtures should be vandal-resistant. It is vital that repair and replacement of defects or worn-out bulbs be immediate. In addition, prevent trees or bushes from blocking lighting fixtures.
9. You may wish to use timers and/or automatic photoelectric cells. Such devices provide protection against human error, and ensure operation during inclement weather and when the building is unoccupied.

A security professional should be contacted to help you with decisions on location and the best type of lighting for your individual institution.

General Target Hardening

One function of security devices, lighting, fences, etc., is to make your facility look less inviting to a potential attacker. The more uninviting your institution is to such an attacker, the less likely the attack. This is called "target hardening." While an institution should not reveal the details of its security measures, providing a potential attacker with clear evidence that a security system is in place will often deter an attack before it happens. Some examples of target hardening:

1. Signs indicating the presence of an alarm system.
2. Visible security patrols and/or vehicles.
3. Well-maintained fence lines and lighting.
4. A general appearance of a well-maintained facility.
5. Regular presence of local law enforcement on or near your grounds.

Relationships with Emergency Personnel

It cannot be overemphasized that developing relationships with your local emergency responders - police and fire - will enhance the security of your institution. We believe that this is a critical component of any effective security program.

The following are some suggestions on how to build relationships with your local emergency responders. In many cases, your ADL Regional Office can help facilitate these relationships.

Law Enforcement

1. Have a meeting with the local police commander (precinct captain, substation commander, etc). He/she will be more than happy to meet with you. The meeting should include the local commander, and the lieutenant or sergeant responsible for patrol officers in your area. Ascertain what information they need from you so that they may more effectively provide service. This is important because all these officials have limited resources, and you need to demonstrate that you are not only asking for assistance, but that you are supportive of their efforts and are an active participant in your own security.
2. Meet the patrol officers who will be the first responders to any call from your institution. This may take three meetings - including one night meeting - given changing shifts. The reason for this is to seek to develop a personal relationship and an understanding on the part of officers of the role your institution plays in the community.
3. You may wish to offer your facility as a place for officers to use the restroom, have coffee or even as a quiet place to write reports.
4. During special events (including holidays), it is appropriate to keep your local police department informed as to the times and the nature of your event. It is also useful to advise them of times when people are typically walking or driving to and from your institution.

5. Most police departments have crime prevention officers. As we have said elsewhere, seek their advice on your security plan and any security issues they may observe. Note: although this is changing in light of September 11, crime prevention officers are typically concerned with issues of burglary, theft and the security of your institution from those who seek pecuniary gain. While there is a great overlap between an anti-crime audit and a security audit, they are not synonymous.
6. If your local department has a special weapons and tactics team (SWAT), consider having a SWAT officer map your institution and its property and determine what information would be helpful in the unlikely event that a SWAT team is called to your institution.
7. It would also be useful to have a member of the bomb squad talk to your appropriate staff. This would also be a good opportunity to consult with the bomb squad regarding the information they need from you to be effective. You may need to go through your local police department in order to have access to a bomb squad.
8. If appropriate, consider volunteering your site to serve as a location for SWAT or bomb squad training.

Fire Department

1. Meet with local fire officials, such as the chief of your local fire department, a member of the fire marshal's staff, as well as the commander of your local station. As with the police department, recognize that these officials are under budgetary and time constraints but should be willing to have someone review your facility and its plans.
2. It is also advisable to meet with local EMT personnel to help create a medical emergency plan. Things to consider:
    a. First aid and CPR training for staff; and
    b. An emergency medical kit appropriate for your institution (including the acquisition of an Automatic Defibrillator machine).

In all cases, recognize the extraordinary service all of these individuals provide our communities. Working with them will enhance their ability to serve your needs.

Finally, it is worth having and sharing plans of your facility with local emergency responders. If they are unwilling or unable to keep them on file, consider having them stored in a secure nearby, off-site location for quick access during an emergency.

Explosive Threat Response Planning: Bomb Threats, Mail Bombs, Truck Bombs and Suspicious Objects[3]

This chapter will help you develop an Explosives Threat Response Plan, dealing with Phone Threats, Mailroom Security, Suspicious Objects and Car/Truck Bombs. As with any aspect of security planning, assistance from professionals is advised.

Telephoned Bomb Threats[4]

The bomb threat is an all-too common form of harassment against communal institutions. Responding to such threats requires careful planning and rigorous practice. This chapter will guide you through some of the key elements of an Explosive Threat Response Plan (ETRP). It deals exclusively with explosive threats that are telephoned in or devices that are discovered; other sections of this booklet deal with mailed explosives.

There are essentially five stages your ETRP should address:

1. *Pre-threat.* Physical security, planning and practicing.
2. *Receipt.* The immediate response of personnel receiving a threat.
3. *Evaluation and decision.* The point at which the threat is evaluated.
4. *Response.* Setting in motion an organizational response, from ignoring the threat to searching for a device to evacuating the building.
5. *Information and Post-Incident.* How the organization handles everything from informing constituency of the status of the incident to how an organization recovers from disaster to post-incident review.

---

[3] *While this entire booklet deals with general security guidelines, it is worth mentioning that this chapter deals only with the outlines of an Explosive Threat Response Plan and offers general guidelines only. The ultimate decision on how to handle any explosive threat must be made by the individual responsible for the threatened facility. However, for the vast majority of institutions, we recommend immediate evacuation upon receipt of a threat.*

[4] This section adopted from Bureau of Alcohol, Tobacco and Firearms, Bomb Threats and Physical Security Planning, ATF P 7550.2 (7/87).

PRE-THREAT

Physical Security

It cannot be overstated that the best way to secure your institution from explosives is to have an adequate physical security plan in place. By taking all responsible steps to prevent the introduction of an explosive into your environment, you place yourself in a much better position. The first step in creating an ETRP is having a physical security plan that will help prevent the planting of a device. Of course, since no physical security plan is foolproof, it behooves even the most secure institution to have an ETRP.

Tips on explosive-specific physical security:

1. Offices and desks should be kept locked, especially those that are unused. . Utility and janitorial closets should remain locked at all times, as should access to boiler rooms, mail rooms, computer areas, switchboards and elevator control rooms.
2. Identify and secure potential hiding spaces for explosives. It is important to note that a device does not have to be large to cause severe physical and psychological damage.
3. Trash receptacles, especially dumpsters, should be kept locked, inaccessible to outsiders and/or far away from buildings. The areas around these items should remain free of debris.
4. Cars and trucks should be required to maintain a safe, 300-foot setback from the facility. If no parking setback is possible, consider allowing only properly identified vehicles owned by staff or leadership to park closest to the building.
5. Shrubs and other plants and trees should be trimmed so as not to provide a hiding space for explosives.
6. Employees should be encouraged to maintain tidy work areas so that they or their coworkers will notice if something is out of place.
7. Flying glass is a grave source of danger in the event of a blast. Consider minimizing glass panes or coating with shatter-resistant film.

8. More than one exit may be damaged in a sufficiently large blast. Have several alternative escape routes.
9. Examine your local area to determine if you are at risk from a neighboring institution that may be targeted. Other Jewish institutions, political offices, medical facilities where abortion services are provided, and corporate offices are such possibilities.

An ETRP requires that you understand precisely how your local law enforcement agency will respond to explosive threats. In some areas, the police (or explosive unit) will not respond to such a threat until a device is discovered. In other areas, the police (or explosive unit) may respond to a called-in credible threat, but will not search a facility without a staff member present. This information is absolutely critical to your planning.

Creating the ETRP

As discussed elsewhere in this book, planning includes assessment, plan creation and implementation. It is worthwhile to review these steps, but we encourage you to re-read the chapter on creating a security plan specifically with your ETRP in mind.

- Assessment includes marshaling all of the information resources available to better understand your institution's risk and realities.

- Planning includes many elements, but most critically, it is vital to bring your local police and explosive squad unit into the picture (reminder: you may not have access to a bomb squad. Your local police department or ADL Regional Office may be able to help you reach them).

- Implementation will be discussed in greater detail below, but it bears mentioning that without role-playing various scenarios, drills and reevaluation of your plan, your plan becomes stale and loses considerable value.

Once you have developed a plan, it is essential that all personnel who need to implement have copies and are drilled on it. We suggest creating a checklist which will guide all parties through their required steps.

Some basic considerations for the ETRP:

1. Determine to what extent a bomb squad is available to you and at what point they will assist you.
2. Set up a chain of command.
3. Establish procedures for setting up a command center, both during and after business hours, (see below).
4. Determine what primary and alternative communications are available. Important: cell phones, cordless phones and walkie-talkies (any two-way radio) can detonate a device. Thus, do not use such modes of communications during an explosive-related emergency. Alternatives include hard-wired intercoms and bullhorns.
5. Clearly establish how and by whom an explosive threat will be evaluated.
6. Establish procedures to be undertaken when a threat is received or a device is discovered.
7. Provide an evacuation plan with enough flexibility to avoid danger areas, e.g., the ability to redirect an evacuation if a device is found in a stairwell.
8. Designate and train search teams well in advance of a problem.
9. Establish procedures to establish search patterns and track the progress of search teams.
10. Establish procedures for a search team to record where they have located a device and a method for leading an explosive squad to the site.
11. Have building plans readily available.
12. Establish simple procedures for the recipient of the threat. The sample form attached to the end of this document will help. Note: anyone who answers outside phone lines needs to be aware of these procedures.
13. Review your physical security plan in conjunction with the ETRP.

14. Critically, know your facility. Know what belongs and what does not and be ready to walk through the facility and help police know the difference.
15. In the event of a detonation, after the immediate emergency has passed, you will need to consider plans for continuing your operations. Having insurance information, lists of vendors and constituents and data-recovery capabilities can be very important to that end.

Practicing

As just discussed, a stale plan loses value. It is of utmost importance to role-play, drill, and reevaluate your plan at several stages. Role-playing involves the participation of all decision-making personnel who would be involved during an explosive threat scenario, talking through situations and variations on those situations to determine if the organization's ETRP is both comprehensive and complete.

Fire drills are often mandated by law or insurance carriers. They are a good way to practice your communication and evacuation plan. Adding explosive drills to the mix may require practicing search techniques, establishing a command post, etc. There is very little substitute for actually moving through your institution and getting a sense of how your plan works during a real-time exercise. Practice may not make perfect, but it will help get some of the kinks out of the system and will help turn your paper document into a real plan that people can use in an emergency.

Receipt of Phoned-in Threats

In this section we will deal with the receipt of phoned-in explosives threats. Mail threats are treated elsewhere.

The first step in developing a response plan for receiving an explosive threat is to meet with your local police department or explosive squad. They should be able to tell you what information they want the threat recipient to take.

Telephone switchboard personnel (or all personnel who receive direct calls from outside the institution) should:

1. Remain calm. A calm response may help in getting important information from the caller and it may provide the person making the threat with a human face to the situation.
2. Do not irritate or insult the caller.
3. Try to have a second person listen in on the call. A covert signaling system should be implemented or a recording device installed.
4. If possible, the threat recipient should not hang up after the call. One suggestion: put the line on hold, and use another line to initiate emergency procedures.
5. Keep the caller on the line for as long as possible. Consider asking the caller to repeat information.
6. Record every word spoken by the caller. Use the check-lists provided below, but also try to take detailed notes *even if there is a recording device installed.* Equipment failure and human error are always a possibility with such equipment.
7. Remember: during a bomb threat, use no devices that generate radio signals, such as cell phones, walkie-talkies, etc.

Information to be sought by the threat recipient includes:

1. **IN AN EMERGENCY use the Explosive Threat Call Checklist provided in this booklet**.
2. If the caller does not provide it, ask the caller WHEN the explosive will go off and WHERE the explosive is located.
3. Inform the caller that the building is occupied and that the detonation of an explosive could result in death or serious injury to many innocent people.

4. Pay particular attention to background noises. Listen for the sound of a motor running, music playing, and any other noise which may provide information about a caller's location.
5. Listen closely to the caller's voice. Record that information on the Explosive Threat Call Checklist.
6. REPORT the information immediately.
7. Remain available for questioning by law enforcement.

Evaluation and Decision

► **Command, Control and Communications**

In any emergency, firm lines of command, control and communications are essential.

1. Command, control and communications form the backbone of an ETRP, indeed, of any security plan. It is essential that a decision-maker be identified, that this person have the authority to act, and that the decisions can be effectively communicated to those who need to know them. It is also important to recognize that a designated decision-maker may be unavailable during an emergency (they may be out sick or on vacation or even at lunch or away from the office for a meeting). Thus, it is important to be able to quickly ascertain who is in charge at any given point. Consider having a list of "succession" in the event of an absence. This will enable you to quickly establish a clear chain of command in light of the day's staffing and attendance.
2. You should consider establishing a command center, the place where your decision-makers meet during an emergency and establish command, control and communications. You may wish to have building plans, contact information and other institution-specific critical information stored at this location. A second, alternate site may be necessary if the first site is unsafe or unavailable. Ensure that your command center can be up and running both during and after business hours.

3. Get your command and communications centers (primary and secondary) up and running.
4. Determine likely targets. Produce a master target list and use it in light of the information received in the threat in order to narrow a search.
5. Determine procedures to establish search patterns and track the progress of search teams.
6. Have building plans readily available.
7. Have a roster of all necessary telephone numbers available.

► **Decision Point**

There are three choices the decision-making authority has after an explosive threat is received:

1. Evacuate immediately
2. Search and evacuate as needed
3. Ignore the threat

All things considered, immediate evacuation is likely to be the wisest choice barring some unique aspect of your facility (e.g., a hospital). While such a policy may lead to a loss of time and/or subject the institution to the use of copycat threats as a means to interrupt business and other harassment, given the potential risk to human life and safety we believe immediate evacuation is, by far, the safest policy. Also, you can reexamine your policy if you later determine that it is being used for harassment.

Other reasons favor an immediate evacuation policy. First, you avoid having to make a very difficult decision under extremely trying circumstances. Second, while the statistical probability is that any threat is false, such threats have led to explosives being discovered. Third, your employees and constituents will appreciate your caution -- and may react badly to your institution's ignoring a threat. Fourth, in the absence of an evacuation, an explosive threat caller may feel ignored and choose to escalate.

► Evacuation

Evacuation requires that you:

1. Notify people of the intended evacuation.
2. Conduct the evacuation in a safe orderly fashion.
3. Be flexible enough when creating your plan to allow the evacuation to proceed if normal egress routes are blocked, dangerous, or damaged.

Some tips:

1. Evacuation plans should account for several different scenarios and route blockages.

2. Groups should be led by someone familiar with the path of egress. That person should look for obstructions and explosives while leading others to safety.

3. Safe evacuation distances vary; however, one rule of thumb is if you can see the suspicious device or vehicle, you are too close.

4. It is useful to have a place to bring evacuees in the event of inclement weather. Arrangements with another facility in your area (a school, hospital, nursing home or a supermarket) will allow you to establish a destination for your evacuees. Some institutions have established more than one safe location increasingly far from their facility (one block, five blocks, 25 blocks). In some rural or suburban areas, there may be no large facility for evacuation; a friendly neighbor's house may be the best place to bring young children.

5. There is also a risk from secondary devices (explosives left outside a facility to harm evacuees). At the very least, try to ensure that evacuees are moved a sufficient distance away so as to avoid such a secondary danger.

6. Children and other persons in need of supervision and aid may raise special evacuation concerns and may have special needs upon exiting the building. While this is discussed in more detail in the section on schools, consider having "to-go" bags which contain items needed for those who would face extra hardship during an extended evacuation.

Search

After a threat, your institution will likely have to perform a search for the explosive, either alone or with the help of the local police or explosive squad. Repeating what we discussed earlier: an ETRP requires that you understand precisely how your local law enforcement will respond to explosive threats. This information is absolutely critical to your planning.

Thoughts on conducting a search:

1. If it is safe to do so, everyone should check over his/her own workspace to ensure nothing has been hidden in the work area.
2. It is recommended that you use more than one person to search every space, even if that space is small. (Ideally, several teams of two should be your primary searchers.) Teams can be made up of supervisory personnel, area occupants or specially-trained search teams. While the first two lead to the quickest search, the latter is ultimately more safe and thorough.
3. When searching a room with two people:
    a. The two enter a room or area.
    b. Carefully move to various parts of the room and listen quietly for the sound of a timing device. Understand that that there is a great deal of noise in typical buildings.
    c. The searchers typically divide the room into four heights: floor to hip level, hip to chin, chin to overhead and finally, ceilings and fixtures.
    d. Starting at a single point and standing back to back, the searchers begin to walk the circumference of the room looking for devices in the first height range. Examine everything, including carpeting, ducts, heaters, etc. When the searchers meet, they should proceed to the center of the room and search objects and furniture there.
    e. Repeat these steps for each of the next two levels.
    f. Finally, check for devices that may be hidden in false or suspended ceilings, and check for lights, building framing members (e.g., rafters, studs), etc.

4. Once a room or area is searched, have a way to let others know it is searched. One common method is to mark the wall with tape or hang a "search complete" sign.
5. The outside of your building must be searched. Examine:
    a. Along walls, looking behind and into bushes.
    b. Inside any enclosure, including planters, sheds, etc.
    c. Under and into every vehicle parked close by. Look for a vehicle that sits heavy on its springs, etc. Identify and examine vehicles that do not belong. (*See* chapter on High Holy Day and special event planning).
6. Teams or your general staff should be trained in this technique.
7. Previously, we suggested keeping unused offices and spaces locked. If you have reason to believe that these spaces may have been compromised, you must search these areas. Your command center should have keys and access cards for all areas.

Discovery

1. It is absolutely critical that personnel involved in explosive searching must understand that they are only to look for and report suspicious objects. THEY ARE NOT TO TOUCH, MOVE OR JAR ANY OBJECTS OF CONCERN.
2. Evacuate the building.
3. Searchers must be able to
    a. Report the location of the device.
    b. Give accurate instructions as to how to locate the device.
    c. Describe the device.
    d. Be available to emergency responder units.
4. Note: Open doors or windows to minimize damage from blast and concussion

POST-INCIDENT

SEE CHAPTER ON POST-INCIDENT RESPONSES.

Mail Room Security[5]

Mailroom security follows the same five-part model, above.

1. *Pre-threat.* Physical security, planning and practicing.
2. *Receipt.* The immediate response of personnel receiving a threat or noticing a suspicious item.
3. *Evaluation and decision.* The point at which the threat is evaluated.
4. *Response.* Setting in motion an organizational response.
5. *Post-Incident.* How the organization handles everything from informing constituency of the status of the incident to how an organization recovers from disaster to post-incident review.

PRE-THREAT

The first key to a mailed hazard response plan is to channel all mail and packages through a screening process, to avoid any letter or package escaping formal scrutiny. This includes items received through the postal service, overnight carriers and couriers.

To establish a mail screening program:

1. Conduct a vulnerability assessment to determine if your organization or a particular employee is a potential target (see chapter on security planning).
2. Appoint a mail center security coordinator and an alternate to be responsible for the developed plan and to ensure compliance with it.
3. Establish direct lines of notification and communication among the mail center security coordinator, management, and your general security office.
4. Develop specific screening and inspection procedures for all incoming mail or package deliveries. At the least, develop a method for ensuring that all packages and mail are examined by someone who is able to evaluate them.

---

[5] Adapted from United States Postal Service, Mail Center Security Guide, Publication 166.

5. Develop specific mail center handling techniques and procedures for items identified as suspicious and dangerous.
6. Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process. If you receive a suspicious package, it may useful to call the addressee to see if they are expecting something.
7. Establish procedures for isolating the suspicious package. At the least, identify an isolated room or area to place suspicious items to hold them until law enforcement arrives. The room, ideally, should have windows that open in order to allow fumes or the pressure wave from an explosion to escape. (Do not place the device in cabinets or drawers).
8. Conduct training sessions for mail center, security, and management personnel to ensure that all phases of a mail bomb screening program work.
9. Conduct training for all employees of the institution to look for suspicious mail and packages.
10. Conduct unannounced tests for mail center personnel.

Depending on the level of risk your institution faces and the resources available to it, you may wish to set up an isolated screening room and have your screener wear rubber gloves and a HEPA face mask to prevent biological or chemical impact.

Receipt a*nd* Evaluation and Decision

All letters and packages should be hand-sorted and screened for the following indicators:

1. Excessive postage
2. Misspelled words
3. Addressed to title only (e.g., President)
4. Rigid or bulky
5. Badly-typed or written

6. Strange odor
7. Lopsided
8. Oily stains on wrapper
9. Wrong title with name
10. Protruding wires
11. *Note:* Do not presume that a mail bomb will necessarily meet any of these criteria. Your observations and intuition are two vital elements in identifying suspicious packages.

Since the most likely person to identify a mail bomb is the intended recipient, all employees should also receive training about what to look for.

Response

Depending on the risk identified, once a suspicious letter or package is identified, a number of steps should take place.

Explosives:

1. Handle the mailed package with extreme care.
2. Do not shake or bump.
3. Do not open, smell, touch or taste the package or its contents.
4. Isolate the package.
5. Enact internal emergency procedures (e.g., evacuate).
6. Call law enforcement.

When isolating the package, it is best to place the container in a room with open windows (to deflect the blast). Do not place the container in a room that has glass walls or doors.

If you suspect that the suspicious package contains biological, chemical or radiological hazards (e.g., it is warm, has strange odors or it contains suspicious powders), then consider the following additional precautions:

Radiological Hazards:

1. Limit exposure -- do not handle
2. Distance yourself and others (evacuate area)
3. Shield yourself from object
4. Enact internal emergency procedures (e.g., evacuate).
5. Call emergency responders

Biological or Chemical Hazards

1. Isolate – do not handle
2. Distance yourself and others (evacuate area)
3. Enact internal emergency procedures (e.g., evacuate).
4. Call emergency responders
5. Wash your hands with soap and warm water

Post- Incident

SEE CHAPTER ON POST-INCIDENT REVIEW

Truck and Car Bombs

Without extensive physical alterations and an extensive security program, defending against truck and car bombs is very difficult. Nevertheless, individual awareness as well as those physical security precautions your institution may take represent an important improvement over doing nothing at all.

Truck and car bomb prevention is a matter of physical security first, and search and evacuation second. Your key defenses are excluding potentially dangerous vehicles from your institution and, if they are admitted to the grounds, keeping them far enough away to prevent damage.

Ideally, all vehicles entering your facility's grounds should be scrutinized before being admitted. While it is much less than ideal, it is still significantly better than nothing to scrutinize vehicles once they are on the grounds or parked.

Truck and car bombs might be identified by the outward appearance of the vehicle and the behavior of the driver. Suspicious facts include, but are not limited to:

1. The person driving the vehicle does not enter the facility, but rather runs or walks away.
2. The car or truck appears to be sitting very low on its springs (indicating great weight).
3. The car or truck is parked illegally or too close to your building. Your facility should restrict parking closest to the building. In an urban environment where on-street parking is close to the facility, consider making a request to the local police department for no-parking designations. Your institution may consider adding physical barriers (cement barriers) between the street and your facility.
4. Note that older cars and trucks are more likely to be used in a car bombing (as are rental vehicles). Be wary of any type of vehicle that appears to have been abandoned (e.g., inspection sticker, registration, or license plate expired or missing, etc.).
6. Information had been received from the FBI that Al Qaeda operatives discussed attacking Jewish institutions using bomb-laden fuel trucks. Institutions should be extremely alert to fuel and tanker trucks parked near their facilities. The police should be called immediately if any doubt exists about the legitimacy of such trucks (e.g., no fuel delivery expected or such deliveries are not expected at your institution or are atypical of the neighborhood).

None of these behaviors are perfect indicators of the potential for violent behavior --and many are consistent with perfectly innocent behavior -- however, they are clues worth considering.

Incremental Steps for Truck Bomb Security

1. Seek to restrict parking closest to building (perhaps no parking at all or limited to staff/key lay leader vehicles). You may choose to use a windshield identification sticker to determine quickly who belongs and who needs further scrutiny.
2. Train staff and security to be aware of the possible appearance of vehicles used in these incidents.
3. Use barriers, gates, etc., to prevent access to the facility by non-authorized persons.

Recognizing and Dealing with Unwarranted Interest in Your Facility

Many terrorist organizations first engage in surveillance on their potential targets. Thus, we should pay serious attention to anyone attempting to photograph or study our facilities - especially in the days and weeks leading up to the High Holy Days or other special events.

Someone examining your facility (or looking closely at the people arriving at or leaving from your building) should be cause for concern. If you spot someone you believe may be doing surveillance on your facility:

1. Call the police immediately. It is crucial that the dispatcher/911 operator be given all available information, starting with the fact that the location is a Jewish institution, and its exact address/location. Other important items would include a description of the suspicious individual, approximate height and weight, what clothing he/she has on, type of car and license plate number if one is observed, and any unusual characteristics that would make the person or persons easy to identify.
2. Consistent with your safety and personal comfort level, consider photographing the person doing surveillance. If the institution has video cameras that are actively monitored make sure the operators know what to look for and to get film

of the incident. Every institution should be encouraged to have a camera available to take photos of suspects. Inexpensive disposable cameras will suffice but do require that the photographer get closer to the subject.

3. If the person leaves before police arrive, you may choose, consistent with your safety and personal comfort level, to approach the individual and inquire as to why he or she is taking photos of the location. The response may be "none of your business, I can take pictures of whatever I want." This is true (unless the person is trespassing) but will have the benefit of placing the person "on notice" that his or her actions were observed. Get a picture of the subject/car as he or she leaves.
4. Even if the person leaves, police should be informed and given a report. If the responding law enforcement officer refuses to take a report, call ADL. Also, here is where preexisting relationships with police help: contact the person you already know. If a dispatcher does not consider this an emergency, inform him or her that you feel threatened and require assistance immediately.
5. Ensure that your staff knows all relevant facts and so can identify the person or persons if they return.
6. Your safety is of paramount importance. Remember: call the police first and act to take pictures, get license information, etc., only if you are confident that it is safe to do so.

Suspicious Objects

Prior to the start of services or events and at the beginning of each day, ushers, security guards and others should walk the perimeter, including parking lots and if possible, rooftops, as well as inside the facility. They should do this in order to refresh their memories as to what belongs and what does not. During the holiday or event, ushers and security guards should periodically patrol the facility.

If you come across a suspicious item:

1. **Leave it alone.** Do not move it or touch it.
2. **Establish Ownership.** Ask people in the immediate vicinity if they own it.
3. **Evacuate.** If you decide it may be an explosive device, evacuate the vicinity (*rule of thumb*: after you have evacuated, if you can see the device, you are too close).
4. **Call Police.** Call the police immediately -- but do not use a cell phone or any other electronic device (bombs may be triggered by radio signals)

A Brief Look at Weapons of Mass Destruction (WMD)

This chapter is intended to provide general information in an effort to enhance your knowledge and to assist in efforts to recognize potential WMD-related threats or incidents. It is adapted from a fact sheet provided by the Federal Bureau of Investigation. Other government sources, such as the Federal Emergency Management Agency can provide additional information about how to respond to a WMD incident. This information is not exhaustive.

OF CRITICAL IMPORTANCE: WMD's are extremely hard to manufacture. They are also extremely difficult to deliver effectively. Finally, most so-called weapons of mass destruction will have a limited effectiveness range. Thus, your risk from WMD's is likely to be minimal. However, it is still important to understand WMD's and be able to prevent and react to their use.

Chemical, biological, and radiological material can be dispersed in the air we breathe, the water we drink, or on surfaces we physically contact. Dispersion methods could include placing an open container in a heavily used area, using conventional garden/commercial spray devices, or detonating an improvised explosive device to disseminate chemical, biological or radiological material.

Chemical incidents are characterized by the rapid onset of medical symptoms (minutes to hours) and easily observed signatures (colored residue, dead foliage, pungent odor and dead insect and animal life). In the case of a biological or radiological incident, the onset of symptoms may take days to weeks and there are typically few characteristic signatures.

In all cases, being alert to the following could assist law enforcement and emergency responders in evaluating potential threats.

Potential Indicators of WMD Threats or Incidents

1. Unusual packages or containers, especially those found in unlikely or sensitive locations, such as near HVAC or air-intake systems.
2. Unusual powders or liquids/droplets/mists/clouds, especially those found near air-intake/HVAC systems.
3. Indications of tampering in targeted areas/equipment (i.e., locked ventilation/HVAC systems; stocks of food; water supply).
4. Reports of suspicious person(s) or activities, especially those involving sensitive locations within or around a building.
5. Surveillance of targeted areas, including but not limited to hotels, entertainment venues, subway systems, aircraft, water sources, office buildings, apartment buildings. Theft of chemical products/equipment.
6. Dead animals, birds, fish, or insects.
7. Unexplained/unusual odors. Smells may range from fruity/flowery to sharp/pungent, garlic/horseradish-like, bitter almonds, peach kernels, and newly mown grass/hay (realizing that some of these smells have perfectly innocent explanations).
8. Unusual/unscheduled spraying or discovery of spray devices or bottles.

Protective Measures:

1. Maintain a heightened sense of awareness.
2. Place an increased emphasis on the security of immediate surroundings.
3. Conduct periodic inspections of building facilities and HVAC systems for potential indicators/irregularities.
4. Review emergency operations and evacuation plans/procedures for all locations/organizations to ensure that plans are up-to-date.
5. Promptly report suspicious activities to appropriate law enforcement authorities.

Emergency Procedures - Potential Threat Identified/Confirmed

1. Maintain a safe distance/evacuate area (if outside, move to upwind location; if inside, keep outside doors/windows closed).
2. Call your local 911 (law enforcement and public safety personnel) after reaching safe area.
3. Do not handle or disturb suspicious objects.
4. Remove possibly contaminated external clothing (including hats, shoes, and gloves).
5. Follow emergency operations plans/instructions from emergency response personnel.

Note: In an effort to prevent spreading contamination and to ensure appropriate decontamination and medical treatment, after moving to safety, do not leave until instructed to do so by law enforcement.

Armed Assaults and Suicide Bombers

These are, without question, the most difficult topics to consider and take action against. Statistics indicate that the chance of a suicide bomber or armed invader attacking your institution is remote. However, if such events occur, they are potentially very deadly and require the institution be able to react appropriately. In sum, while the risk of such events is very small, the damage they can do is tremendous.

A word of caution: no security manual can adequately provide a response plan to either of these phenomena. What we attempt to do here is raise the issue, providing some insight into the phenomenon, so that you and your key staff can have a serious discussion of – and effective role playing about – possible responses. It goes without saying that such responses will involve very hard choices made in a very compressed time period with serious repercussions.

Armed Intruders

This is an issue that your local police department has likely considered. It is important to involve them in these discussions.

While it is unlikely that you will ever face this situation, and while there is not a great deal you can do, the only thing worse than facing an armed intruder is facing one without having prepared at least some response. Some thoughts:

1. It is vitally important to communicate with staff in order to direct a lock-down or to lead people to evacuation routes away from the area occupied by the gunman. As discussed above (in dealing with explosive threats and elsewhere), quickly establishing the three "C's": command, control and communications are all critical here.
2. Fire alarms should not be activated as they cause panic and may lead people to move directly into the path of the intruder.

3. You should have a way to contact your local police department that does not require your returning to an area of danger. Thus, consider having a cell phone in the facility at all times.
4. When speaking with a police dispatcher, try to speak calmly and quietly, informing the dispatcher of the danger facing the institution. If shots are being fired, it is vitally important that you inform the dispatcher that there is an "active shooter" and that immediate intervention is required.
5. Lockdown may be preferable to evacuation. During a lockdown, students and faculty should be directed to lock their room doors and windows and move away from windows and other glass. You may wish to develop a method of signaling officials that a room contains locked-down persons. This may be as simple as placing green or red paper in a window, the former to indicate that there are people inside who are well, the latter that emergency attention is required.
6. This is yet another opportunity to state the importance of a previously established relationship with law enforcement.
7. Establish a way for employees to communicate with you that they are safe. One possibility is to use a muster point (though it may not be practical in light of the panic that follows an armed intrusion). Other possibilities include using a cell phone to contact a nearby institution known to your staff that can begin to take names. At the same time, you should keep an off-site staff list.

See the chapter, Considerations for Schools and Summer Camps, for further discussion of lock-downs and evacuation pertaining to children.

Suicide Bombers

Considering the possibility of suicide bombers is perhaps the most horrible security issue you will be called upon to consider. THERE ARE NO EASY, SET-PIECE ANSWERS TO THIS THREAT.

Role-Playing

We strongly recommend that members of your security committee, the board of directors and your "front line" personnel - greeters, ushers, hired security guards or their managers and/or others – role-play as a team possible threat scenarios and responses. To do this, you may wish to determine whether any member of your institution has experience in this field. Otherwise, you and a small group should develop scenarios involving the approach of a suicide bomber; his/her attempt to gain entrance, and the possibility that he/she may actually gain entrance to your facility. It is important to alter the nature of the scenarios and carefully analyze lessons learned. For instance, if role-playing leads you to try to engage the suspicious person in conversation while someone else dials 911, you need to determine (a) who will dial 911 or contact emergency personnel, (b) who will make the decisions, and (c) what you will say to the person to try to engage him or her.

Possible Indicators of a Suicide Bomber

Suspicious people may often be identified by their behavior. While no one behavior is proof that someone is planning to carry out an attack (and many of the following behavioral indicators are perfectly consistent with innocent behavior), and while no list could ever be complete, these factors can help you assess whether someone poses such a threat.

Behavioral Factors to Consider:

1. Nervousness, nervous glancing or other signs of mental discomfort/being ill-at-ease. This may include sweating, "tunnel vision" (staring forward inappropriately), and repeated inappropriate prayer (e.g., outside the facility) or muttering. This may also include repeated entrances and exits from the building or facility.
2. Inappropriate, oversized, loose-fitting clothes (e.g., a heavy overcoat on a warm day).
3. Keeping hands in pockets or cupping hands (as if holding a triggering device).

4. Constantly favoring one side or one area of the body as if wearing something unusual/uncomfortable (e.g., a holster or a bomb belt or vest). Pay attention to a person constantly adjusting waistbands, ankles, or other clothing. Projected angles under clothing may also be indicative of a firearm, e.g., at the waist or the ankle. Suicide bombers have been known to repeatedly pat themselves to verify that the bomb vest or belt is still attached.
5. Carrying packages.
6. Security personnel should be told, when possible, to observe people as they exit their cars; by watching how they adjust clothing and how they approach the building, looking for signs that a person might be carrying a weapon, etc.

Again, many of these, especially the last, are often consistent with perfectly innocent explanations.

The most important thing is to be observant. For example, Israelis have become aware that some suicide bombers shaved off beards prior to committing their acts, thus leaving unusual facial tan lines. (In Israel, the majority of bombers have been males, 18 – 27.) Some also anointed themselves with scented oil, which may be obvious to someone in their vicinity.

Responding to a Perceived Threat

While no one factor is a certain indicator of a problem, once a problem is identified, ushers and security personnel have three options: do nothing, investigate and decide whether to take emergency steps, or immediately take emergency steps. <u>This is a decision only you can make in light of the circumstances, your personal comfort level and safety considerations</u>.

You must, at all times, be aware of the threat to worshipers, students, or others if the individual about whom you are concerned gains access into your facility.

If you choose to investigate, one technique is to greet the person in a friendly fashion, asking, “Can I be of assistance?” Evasive or unusual answers may trigger your emergency procedures. Excuse yourself and initiate your procedures, perhaps by using a predetermined code-word with your colleagues.

If you believe that a person poses a threat, we urge you to try to prevent entry to the facility.

If you choose to call 911, make sure the dispatcher understands the emergency nature of the call and the need for a law enforcement response without sirens. Off-duty officers are generally armed and are aware of security procedures.

If you remain suspicious, trust your instincts. Even if the person leaves immediately, call the police.

Disturbed Individuals

One somewhat related problem is dealing with what might appear to be a disturbed individual. Only you can make a decision on how to proceed in light of given facts and circumstances.

This is a tough call. We suggest excluding from your facility any individual who you think poses a security risk. However, if you choose to admit the person to the facility pending assistance (e.g., arrival of police) it is important that the person be monitored (for example, invite the person to sit in an aisle seat). Assign an usher or employee to monitor the location of the individual and his or her actions to determine whether any additional, immediate action is necessary.

Considerations for Schools and Summer Camps

Schools

By and large, the entire contents of this manual apply to religious schools. However, some specific recommendations may be helpful.

Hebrew schools and Jewish day schools represent a key arena of concern. Parents are keenly aware of the visibility of many these schools and past targeting of Jewish institutions by those who would do harm. Therefore, pressure is brought to bear by parents - often in a highly emotional and unstructured manner - demanding that schools spare no expense to ensure the safety of their children. It behooves the principal/director, staff and lay board to consider the implementation of a serious, on-going security program, if one is not in place, before events - which typically happen outside the institution - result in rapid, ill-considered and potentially costly steps.

This chapter will not focus on the cause and prevention of student-initiated violence. However, some of the items discussed may be applicable.

Everything we have said about building relationships with police applies here. Indeed, your location may be considered ideal for SWAT or other police training exercises.

Physical Security

1. Follow the steps discussed elsewhere in the manual. However, in conducting your assessment /audit, recognize that Jewish day schools and Hebrew schools are attractive targets to those who may wish Jewish communal institutions harm. They may also be targets of those who wish children harm, in general.

2. It is vital that all staff wear photo identification and that all visitors understand that visitor's ID must be worn without exception. There must be 100 percent compliance by all staff and visitors. Your institution should decide how that

compliance is to be achieved. Failure to comply with the badge program diminishes, both in reality and in the eyes of key constituencies, the commitment of the institution to the security of those in their charge.

Special Evacuation Concerns

1. You must provide for sufficient and age-appropriate supervision.
2. Responding emergency personnel will need to know the numbers and ages of the children who are involved as well as the numbers of staff involved.
3. An effective and immediate telephone chain must be established to prevent panic on the part of parents hearing of an evacuation or threat.
    a. Information for the telephone tree should be simple so as to avoid confusion and prevent muddling of information as it is passed person-to-person.
    b. Information should be calmly conveyed.
    c. It is extremely important to let parents know where the children are being taken as well as when and how the children can be picked up. NOTE: it is recommended that parents as well as staff be informed at the beginning of every school year of the evacuation plans an institution may have. Remember, rumor and innuendo are the most toxic forms of communication.
4. Children, especially young ones, need to be taken to a sheltered environment. This can mean any location that is sufficiently far from your institution to ensure safety and is protected from the elements, etc. Examples may include a neighboring school, church, business, etc. You should, of course, make plans in advance to use such a facility. You may need to work to find a facility or combination of facilities that are open during your entire range of business hours.
5. Be prepared for the possibility that staff or children may have to remain in that location for a number of hours. Consider the desirability of creating “to go” bags - e.g., disaster preparedness kits - for each classroom. Such kits could be readily taken by each teacher in any kind of emergency, particularly those requiring

evacuation. Each bag might have a contact list for every child in the classroom (possibly along with a secondary, out-of-area contact), as well as some food, water and sunscreen. Such a kit would also be useful in lockdown situations.

Lock-down

There are a number of reasons to initiate lock-downs, the most serious of which is the presence of a dangerous intruder where clear lines of safe evacuation are unavailable. Other circumstances include nearby police operations (which speak to the need for police to know your location and function).

A lock-down is a procedure whereby students and staff lock themselves into their offices, classrooms or other safe areas until danger has passed. Were a lock-down to be initiated, the first issue is communicating that fact to staff and students both in the classroom and throughout the campus. Students may be away from buildings, on a field, walking between classes, etc. They must be quickly informed and know to go into the nearest classroom or office. This presents a very confusing situation because (a) students who are unknown to a teacher may seek entrance into a class and (b) may make accounting for students' whereabouts very difficult.

Some considerations:

1. Can your rooms be locked from the inside?
2. Do classrooms have windows large enough to present a danger to those inside the rooms? If so, is there a place to hide?
3. Are there means of communication from classrooms to either the main office or the outside? If not, is there a procedure (possibly using colored cards) to inform police that all individuals in your room are safe or, conversely, that assistance is required immediately? The ability to convey such information may save lives. WHATEVER SYSTEM YOU USE, IT MUST BE SHARED WITH, OR, BETTER YET, DEVELOPED IN CONCERT WITH LOCAL POLICE.

4. Are your rooms stocked for what might be an extended stay? Consider having water, food and perhaps some form of sanitation facilities available.

Specialists

We have recommended elsewhere in this manual that you may wish to consult with a security professional. Your local public school district may have such a professional on staff or be willing to make a recommendation.

Telling Parents about Security Plans

Parents often will ask in great detail about your security plans. The information provided to parents should be sufficient to calm concerns, but should not be so detailed so as to potentially impact the effectiveness of the security program. One way to manage this issue is to have a parents committee that is fully briefed and able to provide assurances to other parents.

Note: security plans and evacuation information should not be posted on Web sites or presented in other public arenas.

Summer Camp Security

Summertime is not normally associated with security concerns, and those who work in as well as attend summer camps anticipate an enjoyable summer experience. And with some careful planning, summertime can remain enjoyable and safe.

The elements of a security plan for summer camp deal with

1. Physical security
2. Information and communication
3. Emergency planning

As in all institutions, one key element in security is the ability of management to establish command, control and communications in an emergency. While this is made more

difficult given the nature of camps (they can be remote, or have children and adults outside playing on many fields at once, etc), planning will make this possible and thus is an issue that camps can go a long way to meet.

Physical Security

While most of the considerations about physical security addressed elsewhere in this book are applicable, summer camps have unique security issues.

Day Camps

Days camps that are contained within the confines of a Jewish institution should be included in that institution's security plan. Even with such a plan in place there may be differences:

1. Young people are outside far more often and for longer periods of time
2. Pickup and drop-off times may be more crowded
3. Other uses of the facility may be occurring simultaneously with camp

At the very least, this translates into a need to exercise extreme caution when dealing with access to campers. Specifically, great attention needs to be paid to identifying those who are part of the camp program and challenging (in an appropriate way) those who do not belong.

Suggestions for all camps:

1. Photo identification should be worn by staff and other adults permitted to enter the camp.
2. If any identification is used by campers, it is very important that care be taken not to provide an opening for strangers to talk to the child, for instance, by making the child addressable by first name (e.g., by minimizing the printed name's size).
3. Staff should be carefully trained to report any person who attempts to make contact with campers.

a. Though the majority of staff at a camp are young people, they can nevertheless play a role in challenging unknown individuals, even if it is only sending a fellow counselor to the administrative office to alert officials to the presence of an unknown individual.
b. Young counselors should not approach individuals but should maintain observation from a distance.
c. The issue of how to alert responsible adults is one that must be worked out well in advance of the need and role played with senior counselors.

4. There should be at least one staff member with a cell phone available at all times, especially when campers are away from the main building (e.g., at a sporting field), to enable you to contact emergency personnel (without leaving the campers).

Sleep-Away Camps

Sleep-away camps have all of the challenges of day camps, multiplied by the fact that their responsibility extends 24 hours a day, seven days a week and that they are often located in remote settings.

Given the special nature of sleep-away camps, the following ought to be addressed, perhaps with the assistance of a professional security consultant. As we have said elsewhere, this is an important time to build relationships with local law enforcement. Indeed, it may be prudent to reach out to law enforcement during the "off-season," when these officials and the camp staff are all likely to be less busy.

The following are general considerations for camps, and we note again that a security professional may be required.

1. Signs
    a. Posting. Institutions should clearly delineate their property with signs that indicate that trespassers are not welcome.

b. Directions. Consideration should be given to the appropriateness to providing widely disseminated directions to the camp from public roads, especially if the camp is identifiable as Jewish by name.
c. Internet. Information posted on-line should be very carefully screened. Consider not providing detailed directions to your camp.

2. Access control
    a. All visitors must be directed - both by signs and physical layout - to the main administration building.
    b. While badges or identification may be difficult for campers to wear at all times, all adults should be identified by badge, whether staff or visitor. Staff should, at least, be trained to direct visitors to the administration building and depending on the age of the counselor, to take other steps as necessary.
    c. While it is unlikely that a sleep-away camp is fenced, there should be some method for keeping strangers and vehicles off the property, particularly at night. Consideration may be given to the possibility of fencing or patrolling the most sensitive parts of the camps, namely sleeping areas, and thus dramatically reducing the area that needs to be secured. Note: if a counselor is patrolling, serious consideration must be given to his/her ability to contact a senior counselor (walkie-talkie or even an air horn).
3. Mail
    a. Consider using a mail screening program (see section on mail screening, *above*) but the use of preprinted address labels may facilitate that process.
4. Lighting
    a. Areas and paths used at night should be well lit.
    b. Cabins should be well-lit inside and out, front and back (especially if the cabin backs against the woods).
5. Sleeping cabin security
    a. Cabins should have lockable doors and windows.

6. Evacuation and lock-down procedures

    a. Evacuation procedures need to be worked out well in advance, especially if the camp is remotely located. You may decide that the best place to take children is to a main building, and such as mess hall, recreation hall, etc. If so, consider ensuring that these buildings have sturdier locks and doors.
    b. Consider having the ability to institute a lock-down if necessary.
    c. See section on school evacuation.
7. Training
    a. Staff must be included in training, practice and critique of a security plan.
    b. Refresher training is important as stale information is quickly forgotten.

Information and Communications

There are two types of communications we will consider here: communication of personal information and emergency communications.

Personal Information

All data pertaining to campers, employees, their families and their summer schedules should be treated as very sensitive information, and kept in a secure and locked location. In addition, no information should be provided to any individuals, regardless of their story, about campers, employees, their families and their summer schedules. Such information should be distributed on a verified need-to-know basis only.

Again, camps should review the amount and types of information they post on the Internet. While it is understandable that camps wish to post as much information as possible on their Web sites, they should remember that once data is on the Web site it is impossible to ever "erase" that information from the Internet. If your camp uses a Web site to communicate with parents, consider a password-protected environment.

Cell Phones

Communications in remote locations can be very difficult and intermittent.

1. There should always be at least two forms of communication available, typically a landline and a cell phone (see below). Radios or satellite phones may be required, given the rural location of some camps.
2. At least one staff member should have a cell phone available at all times, especially when campers are away from the main building or areas (e.g., at a sporting field), to enable contacting emergency personnel immediately (without leaving the campers).
3. Sleep-away camps in rural areas - or if day camps are taking day trips into rural areas - may need to consider alternate means of communication as cell phones may not work. Note: even if cell phones work on the main road driving up to a remote area, they may not work once off that road. It is important to let authorities in the remote area know when and where you will be and when you are expected to return as well as inquiring of them about communication in the remote area (there may be nothing). If there is no form of communication available, additional resources (medical, additional counselors, etc) may be needed. At the very least, <u>do not publicize your trip beyond the appropriate camp family</u>. This may require a review of the camp's promotional literature and Web sites.

Intra-Camp Communications

Camps should seek to be able to communicate with all areas, regardless of the remoteness of the location of some facilities. Bear in mind that radios may not be useable if you are dealing with a bomb-threat (radio signals may detonate a device). Consider using a public address system with a prearranged emergency signal or word, bullhorns, hardwires systems, etc.

A Note on Emergency Planning

Again, a critical issue facing camps, especially sleep-way camps in remote locations, is establishing command, control and communications in an emergency. However, as the above discussions indicate, careful planning and consideration can go a long way to reduce this particular concern.

Guidelines for Hiring a Security Contractor[6]

Once a decision is made that your institution has short- or long-term security needs, it should be determined whether limited or complex security requirements are necessary. ADL strongly recommends that each institution undertake security as a long-term, ongoing process. Depending on the nature/complexity of the institution, an assessment by security professionals might be required.

Statement of Work

During holidays or special events where security guards may be required on a short-term basis, institutions should obtain competitive bids as soon as possible. It is essential to check with local law enforcement and other community agencies for recommendations. Further, the institution should define the security contractor's scope of work. All of the following criteria should be met:

- A concise statement describing the security tasks to be performed including the number of days and hours that security is needed. This information should be clearly outlined with the security contractor before security staff is assigned to the site.
- A detailed set of general and particular special instructions. The importance of these instructions cannot be overstated. The institution should not rely on the security contractor to provide them. These instructions should be discussed with and agreed upon between the decision-makers of the institution and the security firm. Contractors are to provide supplemental instructions to their personnel.
- Assignment of one person who will be the security guard's contact, and will greet the security guard upon arrival to ensure that the guard understands his/her role, and among other requirements, has a neat appearance and proper attitude.

[6] Prepared by the San Diego Regional Office's Inter-Agency Security and Safety Committee.

Interactions with Security Guards

First impressions are important in determining how the security guard will perform. It is important to remember that the guard is present to deter and detect unusual or suspicious activity as well as to safeguard property and people. The following are key points that the institution's contact person should discuss with the security guard:

- The security guard will be assessed during the shift for alertness.
- Rules of conduct that enhance effectiveness. For example, no smoking, practical joking, fraternizing, etc.
- The scope of work should be explained and written concise expectations presented as soon as the security guard arrives (keeping a copy for yourself):
    - Institutional contact and how to immediately reach him/her.
    - Requirements of the assignment.
    - Purpose of security during the prescribed times.
    - Layout of the facility.
    - Facility security and/or fire regulations.
    - Any vulnerable areas.
    - Locations of telephones, fire-fighting equipment, fire alarms, emergency exits, etc.
    - Location of stairways and doors.
    - In the event of an emergency (fire, suspicious package, bomb threat, etc.), clear operational guidelines.

Criteria for Security Contractor Selection

As soon as the need for a security firm has been determined on an immediate or long-term basis, a security contractor should be selected. Selecting a company that has valid, current state licenses is essential. To determine the reputation of a security contractor, it is advisable to investigate any history of complaints about the prospective security contractor reported to the state licensing authority. You should be certain that a company is reliable and in good standing.

All of the following criteria should be met:

- Insurance
- Track record/reputation
- Proposal characteristics
- References
- Training
- Equipment
- Costs
- Contract
- Management
- Security guards

For your convenience, please see a checklist.

Insurance

After a security contractor's license has been established, scrutinize the insurance coverage the security contractor provides. The following criteria should be met prior to hiring a security contractor:

- The contractor provides and maintains adequate insurance coverage for your situation.
- Your risk manager (insurance agent) approves of the contractor's coverage.
- Contractor's Broad Form General Liability Insurance covers a minimum of $1 million per incident and $3 million total. The higher the coverage the better. Determine whether the contractor has fidelity bonding and other coverage.
- Workers Compensation Insurance is at statutory minimums.
- The contractor should have adequate Automobile Liability Insurance coverage for all vehicles used.
- Security contractor's insurance covers sexual harassment through their Professional Liability coverage.

- Liability coverage for special equipment provided (golf carts, computer equipment, watch clocks, etc.).
- Contractor's insurance carriers name your organization as "Additional Insured" on their liability insurance policies (or at least, obtain certificates of insurance for the contractor). If so, is there an extra charge for this?
- Your insurance advisor does not object to any of the policy "Exclusions."
- Ask for EMR (Employment Modification Rate) for the last three years (the lower the EMR, the better the contractor's safety performance).

These criteria are important in determining whether a security contractor's insurance coverage is sufficient to meet your needs. A security contractor must both provide security and be properly insured.

Reputation

A security contractor's reputation should be examined to ensure the company has maintained a trustworthy and dependable reputation. To determine the quality of past work, ascertain whether there has been a recent history of valid or successful lawsuits against the contractor filed by clients or employees. This can be learned at your local courthouse or through a local attorney. Consider three main factors when researching a company's history:

- *Negligence*

  Determining possible history involving negligence by the contractor is important. By reviewing liability insurance claims history, your organization should be provided insurance "Loss Experience" or "Loss Runs" by the contractor upon your request. Inquire of the contractor directly whether the company has ever been involved in any lawsuits and whether there has been any legal incident involving their employees while on a client's property during the last 10 years.

  Your lawyer or insurance broker can explain the report and advise you on the significance of each case and report.

- *Workers Compensation Claims*

  Review their listing of worker compensation claims to determine the possibility of patterns of carelessness or inadequate employee safety practices. This report is available from the security contractor and your insurance agent can advise you of the significance of each claim. Again, ask for EMR (Employment Modification Rate) for the last three years (the lower the EMR, the better the contractor's safety performance).
- *Experience/Management*

  First and foremost, you are hiring the guard service management team because, typically, the pool of security guards is the same for all companies. Inquire as to the number of years of service in the security industry of the contractor's president, regional manager and operations management.

  Although not essential, the security contractor should have recently provided similar security service. It is recommended to hire a security contractor that has recent experience similar to the needs of your institution.

Proposal Characteristics

Carefully analyze the proposal submitted by a security agency. The proposal should address the specific security needs at your site and demonstrate that the security contractor has carefully reviewed your needs, giving them full consideration in the proposal. The following are key points that the security contractor should enumerate in a proposal for your institution:

- *Training/Qualifications*

  The proposal should set the minimum qualification as follows: describe the security-related education and training levels of personnel to be assigned at your institution. Security contractors that provide additional education and training are more likely to divulge this information.

- *Staffing*

  Staffing may be regular, rotating or temporary and it is important to know beforehand which personnel you will be dealing with. A permanent staff assignment is always best if it can be obtained. However, security contractors often have difficulty maintaining regular staff as a result of odd shifts, frequently consisting of less than eight hours. You should research the security contractor's history of staff stability and determine excessive turnover or poor relationships with employees. The contractor should also obtain your approval before transferring (or replacing) personnel from your site. To this end, the contractor's needs at other sites should not take precedence over security needs at your site.

- *Description of Supervision*

  Does the proposal describe the exact nature of supervision to be provided? Contractors should be willing to explain clearly how they will monitor and control the quality of security services.

- *Documentation*

  In selecting the best quality contractor, the proposal should describe the frequency of reports and documentation (daily officer activity logs, incident reports, crime reports, officer time sheets, other special reports, etc.). Consistent and thorough written communication is an important output of contract security services and is an important management control mechanism you have over security services and costs.

- *Instructions to Security Guard*

  Carefully analyze whether the proposal includes sample Post Orders or Standard Operating Procedures Manual. This document describes all aspects of job performance at your site, including security guard grooming and decorum, sets the standard of security services, and provides the basis of guard discipline. Ultimately, this document becomes the main basis of legal defense in the event of litigation. The contractor should provide a document that is comprehensive and clear both to you and the security guards.

- *Emergency Procedures*

  The contractor's proposal should describe how his/her guards will function under various emergency conditions. The proposal should demonstrate an understanding and coherent approach to a wide variety of nonstandard, unusual or crisis situations.
- *Equipment Issues*

  If the security guard is expected to patrol your institution when it is closed (holidays, overnight, etc.), he/she should be equipped with a cell phone enabling contact with emergency services if needed. It is important for you to ask what other equipment is standard issue and/or the guard is certified to use. For example, will the guard carry a baton, pepper spray, handcuffs, etc.?

References

References help find quality and reputable security contractors. Client references give invaluable insight as to the reliability and performance of a security contractor and highlight areas of possible improvement. To secure the most qualified and experienced security firm, the following criteria should be met:

- Clients verify a contractor's history of relevant experience.
- Past clients' references verify a contractor's history of responsiveness.
- References indicate contractor's employee turnover rate is lower than or equal to that of industry norms.

Costs

Prospective security contractors should address the following issues:

- How frequently will contractor bill for services rendered? Weekly? Biweekly? Other? Is this convenient for you? 70
- Will it be a flat monthly rate, a uniform hourly rate for all employees or a unique hourly rate for each individual employee? Generally, paying a unique hourly rate for each guard provides clients with the most economy

- Contractor discloses wages to be paid to guards assigned to your site. A good contractor should be willing to discuss openly all cost drivers and the fee or profit margins it expects to earn for the services to be provided.
- Contractor's periodic invoices list wages and bill rates for each guard. Invoice detail provides a good audit trail and shows contractor professionalism.
- How will guard pay increases be handled? Inadequate or stagnant wages are a frequent cause of staff turnover. Wage increases should be proposed in advance by the contractor, based on officer incentive and merit, reflected logically in billing rate adjustment and mutually agreed upon by the contractor and client before implementation.
- Will any additional charges be made for uniforms, equipment, supplies, etc.? Again, these should be proposed, justified, logical, and mutually agreed upon.
- Is the total estimated average monthly cost within your budget? Your monthly guard budget can be calculated using the following formula as a guide:

Estimated average hourly wage rate for security guards in your area	$7
Estimated average monthly hours per security guard	x173
Estimated number of guards at your institution	x2
Estimated cost for security personnel	$2422
Estimated markup factor	x1.65
Estimated total monthly cost to your institution	$3996

The monthly costs to depreciate and maintain necessary security equipment such as patrol vehicles and/or radios should also be reflected in the above budget configuration.

Contract

The security contract ensures the contractor will meet your needs. There are numerous questions and criteria that a security contract should specifically address which indicate the security firm is responsible and dependable. These serve as guidelines to refer to and are enumerated below:

- Does the contractor indemnify you for all security-related liability for which the contractor is responsible? In cases where partial liability is determined by a court of law, does the agreement clearly specify how such indemnifications shall be applied? You should discuss client indemnification of the contractor.
- At contract time will there be a price increase? How much? Why?
- Do you retain the right to terminate the agreement at any time and for any reason? Is this right mutual?
- Is the amount of notice required for contract termination – by the contractor or client – reasonable? Thirty days is the standard.
- Is the agreement sufficiently flexible to meet your needs?
- Does it assure fairness to the contractor and adequate control to the client?
- Can you replace a guard if necessary?

Management

You and the security contractor must share an understanding of the reasons generating the contract. As such, discussion issues should include the following:

- Discuss your desires with management from the outset, allowing the security contractor to communicate with janitors, landscapers and maintenance personnel to create an integrated security team.
- Discuss terms of supervision with the contractor, field and management staff. This ensures that the security personnel know, understand, and comply with your site's written policy manual. If a security guard performs below par, it is important to know that the individual will be counseled, disciplined and replaced by the contractor as needed.

- Once the security guards are in place, you will need to monitor them to ensure that they meet high professional standards, project a professional and alert demeanor, and respond effectively to security-related concerns. It should be required that all that written materials from the security guard (logs, reports, etc.) be clear, complete and usable. These reports should be shared with you.

Deciding What Kind of Security Should Be Hired

It is important to know that hiring a security contractor, whether limited or extensive, armed or unarmed, is a serious business and not to be taken lightly. Different kinds of security guards are appropriate for different situations. An important issue is whether you would like security at your site to be provided by a uniformed or plainclothes guard.

- The main goal of a uniformed security guard is deterrence.
- The main goal for hiring a plainclothes security guard is apprehension.

After deciding what kind of security to hire, you must determine whether the security guard should be *armed* or *unarmed*. There are many costs and benefits to be considered when choosing an armed versus unarmed security guard.

The following should help you analyze the issue and determine what is in the best interest of your institution:

Armed Security Guards

- It is important to determine if hiring armed security guards meets your institution's expectations for security.
- Realize that armed guards may utilize deadly force.
- Determine the training qualifications the security guards have with firearms.
- Determine the contractor's policy on the use of weapons with regard to deadly force

- Keep in mind moral questions when hiring an armed security guard. You should determine whether the members of your institution will accept an armed guard on the premises. Please note that special care should be taken if your institution serves many young people. Schools should be particularly concerned with the message an armed guard conveys to students, parents and staff.
- Consider the cost effectiveness of an armed guard. They are much more expensive than unarmed security, due to licensing and training requirements.
- Decide whether the presence of a weapon may escalate the possible use of force and violence which otherwise may not occur.
- Insurance may adversely affected by the presence of an armed guard.

Unarmed Security Guards

- Use of deadly force is not a desired/required.
- Unarmed security guards often provide the same deterrent as armed guards without the risk of deadly force.
- The protection afforded by unarmed guards is less expensive and incurs less liability and insurance .

Criteria for Security Contractor Selection Checklist

As previously mentioned, when the need for a security firm has been determined on a short- or long-term basis, a security contractor should be selected. The following checklist has been developed to assist you in this process:

Institution Name	
Security Contractor Name	

	Requested	Received	Accepted
Insurance			
Reputation			
Negligence			
Workers Compensation Claims			
Experience			
Proposal			
References			
Costs			
Contract			
Management			
Security Guards			

Post-Incident Review

Once you have handled basic life-safety and emergency response procedures - in other words, as soon as you have established your initial response to a situation - your next task is to appropriately handle communication, evidence, disaster recovery and post-incident reviews.

Command, Control and Communication

As we have explained elsewhere in this manual, it is critical to establish chains of command, control and communication. Besides preventing what may be counterproductive or, worse, deadly confusion during an incident, it will also help you manage those *outside* of the immediate incident, including those who need or want information, such as the media and parents.

1. Designate a single spokesperson for the institution. If it is necessary to have more than one, it is essential that they be carefully coordinated.
2. This spokesperson should be the sole contact point for the media, constituents and anyone else who needs information from the institution.
3. Depending on the nature of the incident, especially if it involves children, the spokesperson might direct constituents to a further contact point.
4. Information should be clear, factual, non-emotional and consistent with law enforcement requirements.
5. The person designated to be your spokesperson should not have other more important duties to attend to during an incident and recovery. In other words, consider how engaged in the emergency and follow-up any potential spokesperson might be.

The media may be interested in your incident. They may also be the most effective way to communicate important information to constituents. Depending on where you are, media may be more or less receptive to becoming a conduit for relaying information.

1. In order to not draw undue attention to the event, you may elect not to call the media. However, media can find out about events without your calling them (they monitor police scanners and have other sources). Thus, though you may wish to avoid media attention, it is sometimes inevitable.
2. When speaking to the media, be clear, direct and honest. Speak in short, declarative sentences. ("The facility will remain closed for the next two days.")
3. Craft your message before you are interviewed. Develop two or three key points and stick to them: e.g., "Everyone is safe, parents should call xxx-xxx-xxxx," "The institution has taken appropriate security measures," "A lawsuit has been filed. In many cases, you can answer any question with these concise, stock statements.
4. Speak to emergency officials about your message, if possible. This is especially true if a crime has been committed. The police may wish you to refrain from mentioning certain facts so as not to taint a jury pool, to help them keep certain facts quiet so that they may determine if a subsequent incident is a copy-cat or not, and/or to ensure that an on-going investigation is not otherwise damaged.
5. You are under no obligation to answer media questions, but note that if a story is to run, you may wish to contribute your point of view.
6. Your ADL Regional Office is available to help you deal with media, for example, by helping you craft a message or work with you on delivering it.

When communicating to constituents

1. Be clear, direct and honest. If possible, be reassuring.

2. Remember that you may be dealing with people who are very anxious and afraid.

Evidence

Consistent with your safety, it is absolutely critical that you seek to preserve evidence of any attack on your institution. This includes:

1. Do not erase or paint over graffiti until the police say you may do so. While the temptation to erase graffiti is a strong one, it is very important that the police are able to examine the graffiti first hand and get evidence from it.
2. Consistent with your safety, take a picture of whatever is your cause of concern.
3. Once you have removed yourself to a safe location, try to record, in writing, every element of the event or incident that you can remember. Write down a description of every mark, note, word or item on a suspicious package or note the license, color, make, and model of a suspicious vehicle. If need be, fill out the bomb threat call sheets when a threat comes in; we urge you to similarly record every detail, no matter how small when another type of incident occurs. Remember: you and other staff members may have differing accounts based on perspective, memory and point of view.
4. Do not handle evidence (e.g., a rock thrown through a window). While sometimes it is advisable to place a suspicious mailed package into a ventilated room, in no other circumstances should you handle a device or other item of concern. See section on explosives.

Disaster Recovery

Disaster recovery may be a part of your post-incident work. Recovery can be made easier if some preparation is done beforehand.

Consider

1. Having off-site, current back-ups of critical data, vendor lists, employee, constituent and donor contact lists, and other mission-critical information. While this may be as simple as someone taking a disk home with them, it is important to recognize that if the disk or data is lost, the information may get into the wrong hands. The security of your backup is vital.
2. Conducting an insurance review to ensure that your insurance is adequate to your needs. Ensure that insurance records are kept with back-up information.
3. Discuss with your attorney the legal aspects of recovery, including discussing whether someone has the legal authority to take emergency steps on behalf of your institution.
4. You may also wish to have worked out plans ahead of time for relocation of students, patients, campers, etc.
5. Anything else that, if destroyed, would cause your institution to cease running. You may wish to factor in any service agreements you have and whether they provide for adequate post-disaster service provision and recovery.

Post-Incident Reviews

Once an incident is over and the recovery operation is in place, it is critical to review the events as soon as possible.

There are four key steps to the post-incident review. In particular, if there is a threat of civil or criminal litigation, you may wish to discuss the following steps with your attorney before proceeding.

1. Review the entire event, minute by minute, in an effort to determine what happened and when. Derive from this activity an assessment of what worked and what did not work. This is not the time to assign blame, but rather to understand what lessons you could learn.

2. Review your threat assessment in light of this incident and the new circumstances your institution may face. For instance, an arson attack may both reveal a previously uncontemplated threat *and* place the institution in the spotlight, creating an incentive for copycats.

3. Revise your security plan accordingly, ensuring that all discovered security needs are filled in.

Practice and drill on the new plan.

Security for the High Holidays and Other Special Events

The High Holy Days and other special events raise special security concerns for the Jewish community.

This guide is designed to help Jewish community institutions prepare for holiday security in a calm and rational manner. Enhanced security does not have to come at the expense of an open and welcoming environment. And it doesn't have to come at the expense of a balanced budget. It requires a commitment from their institution's management and constituency to make security a part of that institution's culture.

General Recommendations

Several thoughts from earlier in this book bear repeating:

1. *Think Security.* Bear in mind that it is everyone's responsibility to keep a watchful eye on their community institutions and we must all take responsibility for security.

- *Leadership* should assess the risks and realities facing the institution and develop a security plan -- seeking professional guidance, if needed. Of course, not all institutions run the same risk, but all run some risk.
- *Congregants and community members* must care about security and let others know that they do. Active cooperation with security procedures and your powers of observation are two of the most important assets you have.

2. Have a *security* (prevention) and an *emergency* (reaction) plan which includes (but is not limited to):

a. Notifying people and evacuating them, if necessary. Designate a meeting place to ensure that everyone is safe.

b. Having a cell phone handy in case you need to call for help from outside the facility. Consider having the local police department's emergency phone number as well as 911 programmed into the phone.

c. Having a person in charge of security and prevention -- and vesting that person with the authority to direct a response during an incident.

3. Speak to local law enforcement about High Holy Day schedules and special events. Invite officers and the fire marshal to the facility for a security review -- especially if the facilities are not the ones you usually use. Ensure that patrol officers are aware of the times during which you will be holding events and during which large numbers of congregants will be walking on the local streets. Consider presenting copies of schedules for distribution at your police department's roll call. A previously developed relationship with law enforcement will help facilitate this.

4. Coordinate ushering and security staff. This is especially important when you are bringing in outside help for the holidays (e.g., off duty police or a security guard). Note: ushers and security should be placed in reasonable proximity to each other so that ushers can quickly alert security to a problem.

5. A facility should have as few entry points as possible (ideally, one). However, remember to obey all fire codes and ensure adequate routes for exiting the building.

6. Ensure that existing safety devices are working and are being used -- especially if you are renting a facility. Video cameras should have tape, parking lot lights should work, etc.

7. Ensure that ushers understand that they play a critical role in security matters (even where there is a security staff) as they are often used to control access to the sanctuary (e.g., by taking tickets) and are in a position to spot trouble early on. Meet with your ushers prior to services to make sure everyone understands their role and security procedures.

8. Pre-event publicity for upcoming events should be looked at in light of security. Potential gains in audience numbers must be weighed against the security concerns created by "going public."

9. For special events where tickets are inappropriate, you may choose to use a guest list or a sign–in book. Regardless of what you choose to use, no one should enter your facility without being greeted and observed. An usher can play that role.

More detailed information on the following topics appears elsewhere in this manual. It is important to consult those sections as well as these.

Other sections in this manual deal with the following related and important topics:

a. Recognizing and Dealing With Suspicious People
b. Recognizing and Dealing with Unwarranted Interest in Your Facility
c. Recognizing and Dealing With Suspicious Objects
d. Recognizing and Dealing with Suspicious Vehicles

DENVER POLICE DEPARTMENT

BOMB THREAT—CALL CHECKLIST

ASK:

1. WHEN? (WILL IT GO OFF)

2. WHERE? (IS IT LOCATED)

3. WHAT? (TYPE OF BOMB IS IT)

4. WHAT? (TYPE OF EXPLOSIVE IS IT)

5. WHY? (ARE YOU DOING THIS)

6. WHO? (ARE YOU)

BOMB THREAT—CALL CHECKLIST

DATE ___/___/___ TIME OF CALL _____

CALL RECEIVED BY: _____ OFFICE: _____ EXT: _____

EXACT LANGUAGE OF THE THREAT: _____
_____
_____

VOICE ON PHONE (Check as applicable):

MALE FEMALE ADULT CHILD ESTIMATED AGE

SPEECH: SLOW RAPID NORMAL EXCITED LOUD FOUL
BROKEN SINCERE ACCENT INTOXICATED IMPEDIMENT

SOFT/HIGH PITCHED DEEP CALM ANGRY RATIONAL

BACKGROUND
NOISES:_____
_____

MUSIC TALKING LAUGHING BARROOM TYPING MACHINES

TRAFFIC AIRPLANES FACTORY TRAINS QUIET OTHER

NOTIFY:
_____
SUPERVISORY OR COMMAND OFFICER

*MAKE A BOMB THREAT OFFENSE REPORT AND ATTACH THIS CHECKLIST

ADDITIONAL
COMMENTS:_____
_____
_____
_____

DPD 199 (7/76)
[Adapted]

Anti-Defamation League

NATIONAL OFFICE (webmaster@adl.org)
823 United Nations Plaza, New York, NY 10017 .....(212) 885-7700

WASHINGTON OFFICE
1100 Connecticut Avenue, NW (Suite 1020), Washington, DC 20036 (natlgov@adl.org) .....(202) 452-8320

REGIONAL OFFICES

ALBUQUERQUE
P.O. Box 21639, Albuquerque, NM 87154 (new-mexico@adl.org) .....(505) 823-2712

ARIZONA
One E. Camelback #670, Phoenix, AZ 85012 (arizona@adl.org) .....(602) 274-0991

ATLANTA (Southeast)
One Securities Centre, 3490 Piedmont Road NE (Suite 610), Atlanta, GA 30305 (atlanta@adl.org) .....(404) 262-3470

BOSTON (New England)
126 High Street, 4th Floor, Boston, MA 02110 (boston@adl.org) .....(617) 457-8800

CHICAGO (Greater Chicago/Upper Midwest)
309 West Washington (Suite 750), Chicago, IL 60606 (chicago@adl.org) .....(312) 782-5080

CLEVELAND (Ohio/Kentucky/Allegheny)
505 Terminal Tower, Cleveland, OH 44113 (cleveland@adl.org) .....(216) 579-9600

CONNECTICUT
1952 Whitney Avenue, 3rd Floor, Hamden, CT 06517 (connecticut@adl.org) .....(203) 288-6500

DALLAS (North Texas/Oklahoma)
12800 Hillcrest Road (Suite 219), Dallas, TX 75230 (dallas@adl.org) .....(972) 960-0342

DC (District of Columbia/Maryland/Virginia/North Carolina)
1100 Connecticut Avenue, NW (Suite 1020), Washington, DC 20036 (washington-dc@adl.org) .....(202) 452-8310

DENVER (Mountain States)
1120 Lincoln Street (Suite 1301), Denver, CO 80203-2136 (denver@adl.org) .....(303) 830-7177

DETROIT (Michigan)
6735 Telegraph Road (Suite 300), Bloomfield Hills, MI 48301 (detroit@adl.org) .....(248) 646-2440

HOUSTON (Southwest)
4635 Southwest Freeway (Suite 400), Houston, TX 77027 (houston@adl.org) .....(713) 627-3490

LAS VEGAS
1050 East Flamingo Road (Suite N339), Las Vegas, NV 89119 (las-vegas@adl.org) .....(702) 862-8600

LONG ISLAND
6800 Jericho Turnpike, Suite 112W, Syosset, NY 11791 (long-island@adl.org) .....(516) 496-0328

LOS ANGELES (Pacific Southwest)
10495 Santa Monica Boulevard, Los Angeles, CA 90025 (los-angeles@adl.org) .....(310) 446-8000

SATELLITE OFFICES

SAN FERNANDO VALLEY, 22622 Vanowen Street, West Hills, CA 91307 (san-fernando-valley@adl.org) .....(818) 464-3220

SANTA BARBARA, 35 W. Victoria Street, Santa Barbara, CA 93101 (santa-barbara@adl.org) .....(805) 564-6670

MIAMI (Florida)
2 South Biscayne Boulevard (Suite 2650), Miami, FL 33131-1802 (miami@adl.org) .....(305) 373-6306

SATELLITE OFFICE

BROWARD COUNTY, 6600 N. Andrews Avenue (Suite 570), Fort Lauderdale, FL 33309 (broward-county@adl.org) .....(954) 938-8188

NEW JERSEY
743 Northfield Avenue, West Orange, NJ 07052 (new-jersey@adl.org) .....(973) 669-9700

NEW ORLEANS (South Central)
925 Common Street (Suite 975), New Orleans, LA 70112 (new-orleans@adl.org) .....(504) 522-9534

NEW YORK (all of New York State except Long Island)
823 United Nations Plaza, New York, NY 10017 (new-york@adl.org) .....(212) 885-7970

OMAHA (Plains States)
333 South 132nd Street, Omaha, NE 68154 (omaha@adl.org) .....(402) 333-1303

ORANGE COUNTY/LONG BEACH
959 South Coast Drive (Suite 374), Costa Mesa, CA 92626 (orange-county@adl.org) .....(714) 979-4733

PALM BEACH COUNTY
700 S. Dixie Highway, Suite 205, West Palm Beach, FL 33401 (palm-beach-county@adl.org) .....(561) 832-7144

PHILADELPHIA (Eastern Pennsylvania/Delaware)
One Penn Center, 1617 John F. Kennedy Blvd. (Suite 1160), Philadelphia, PA 19103 (philadelphia@adl.org) .....(215) 568-2223

SAN DIEGO
7851 Mission Center Court (Suite 320), San Diego, CA 92108 (san-diego@adl.org) .....(619) 293-3770

SAN FRANCISCO (Central Pacific)
720 Market Street (Suite 800), San Francisco, CA 94102-2501 (san-francisco@adl.org) .....(415) 981-3500

SEATTLE (Pacific Northwest)
Plaza 600 Building (Suite 720), 600 Stewart Street, Seattle, WA 98101 (seattle@adl.org) .....(206) 448-5349

ST. LOUIS (Missouri/Southern Illinois)
10420 Old Olive, Suite 208, St. Louis, MO 63141 (st-louis@adl.org) .....(314) 432-6868

OFFICES OUTSIDE THE U.S.

JERUSALEM
21 Jabotinsky Street, Jerusalem, Israel 92141 (israel@adl.org) 011-972-2-566-7741

MOSCOW
36 Noviy Arbat (Office 710), 121205 Moscow, Russia (moscow@adl.org) 011-70-95-207-1794

CANADA
Cooperative Association with the League for Human Rights of Canadian B'nai Brith
15 Hove Street (Suite 210), Downsview, Ontario, Canada, M3H 4Y8 (league@bnaibrith.ca) .....(416) 633-6224

Web site: www.adl.org

Notes