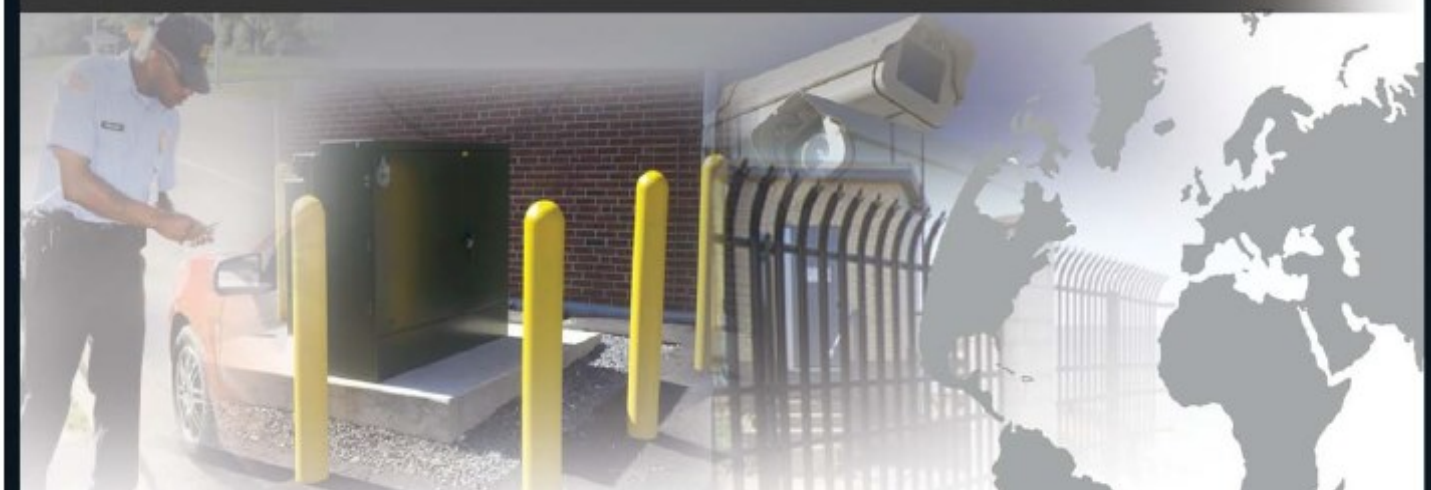
STAS

STATE THREAT ASSESSMENT SYSTEM

Protective Measures for Enhanced Facility Security



(U) "The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

(U) Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery."

Presidential Policy Directive (PPD 21) - Critical Infrastructure Security and Resilience

(U//FOUO) The *Protective Measures for Enhanced Facility Security* was developed to provide a basic understanding of protective measures that may increase security of facilities across the Department of Homeland Security 16 Critical Infrastructure Sectors. This document contains vulnerabilities and protective measures that the State Threat Assessment System (STAS) Infrastructure Protection Working Group has commonly observed while performing site security surveys. The *Protective Measures for Enhanced Facility Security* is divided into sections pertaining to policies and procedures, physical barriers/site hardening, access control, detection, and emergency preparedness.

- Policies establish objectives, priorities, set responsibilities, expectations and accountability for each organization. Procedures are the detailed instructions for staff to carry out that implement a policy.
- Physical barriers refers to the natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials. Site hardening is implementation enhancement of security measures to make a site more difficult to penetrate.
- Access control is the permitting or denying the use of a particular resource by a particular entity.
- Detection is the act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter.
- Emergency preparedness are measures taken in advance of a crisis to reduce injury, the loss of life and property.

The sections include images paired with options for consideration that address certain security attributes or vulnerabilities. This document does not provide an all-inclusive list of enhanced security measures. This document offers options for consideration that may not apply to every facility and should be considered voluntary and non-regulatory in nature. Security upgrades should consider internal policies and federal, state, and local laws before implementation. The STAS recommends that this document be treated as sensitive information, and distribution limited to those who have a valid need to know.

THE CALIFORNIA STATE ASSESSMENT SYSTEM (STAS) FUSION CENTER POINTS OF CONTACT

California State Threat Assessment Center (STAC)

(916) 874-1100, STAC@calema.ca.gov

Central California Intelligence Center (CCIC)

(888) 884-8383, info@sacrtac.org

Northern California Regional Intelligence Center (NCRIC)

(866) 367-8842, DutyOfficer@ncric.org

Joint Regional Intelligence Center (JRIC)

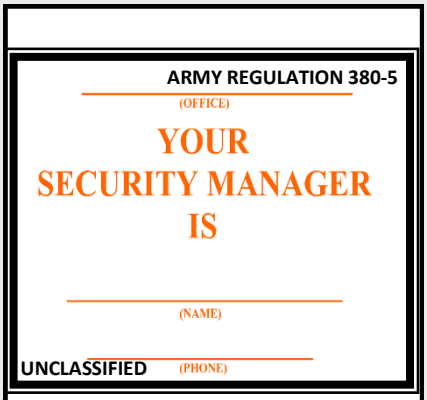
(562) 345-1100, JRIC@jric.org

Orange County Intelligence Assessment Center (OCIAC)

(714) 289-3949, ociac@ociac.org

San Diego Law Enforcement Coordination Center (SD-LECC)

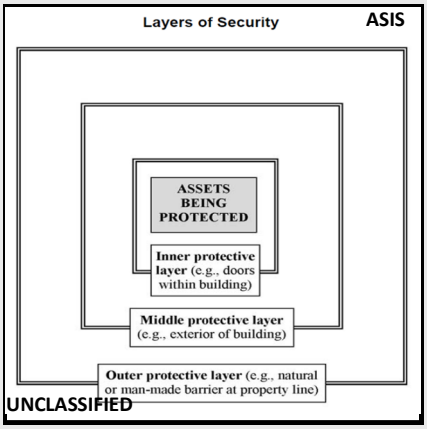
(858) 495-7200, info@sd-lecc.org



Policy and Procedure—Security Manager

Options for Consideration:

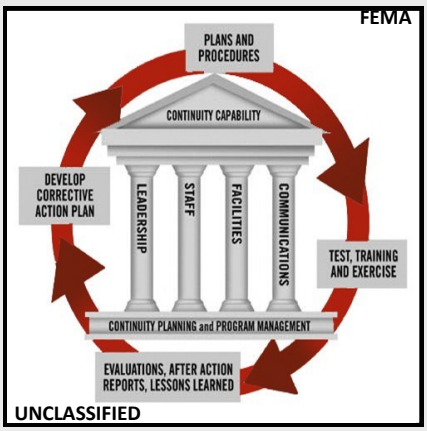
Consider assigning the role of security manager to an employee or volunteer. Assigning responsibility of security management is a good first step to maintaining an effective security program. This person may be responsible for developing baseline requirements, initiating policy, identifying training needs, and establishing continuity of a security program.



Policy and Procedure—Develop a Security Plan/Training

Options for Consideration:

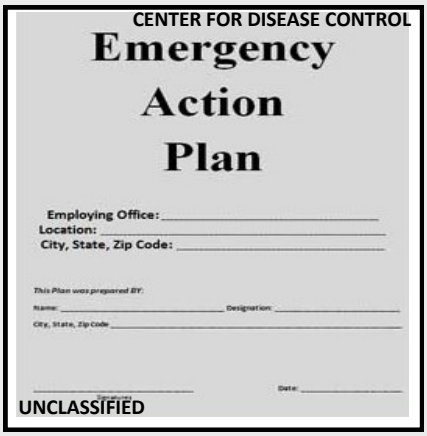
Consider identifying and prioritizing information and critical assets that are essential to maintaining operations. Identify potential vulnerabilities and develop procedures and physical measures to mitigate those vulnerabilities. Ensure that there is a process for reporting security related incidents. Ensure employees are trained on current security procedures and mitigation plans. Conduct additional refresher training as needed.



Policy and Procedure—Develop a Continuity of Operations Plan/Training

Options for Consideration:

Your facility provides vital services to the community, and reliability is a fundamental mission of all critical infrastructure. Discuss potential regional emergencies that could disrupt essential functions. Consider developing a comprehensive plan that ensures essential functions can continue throughout, or resumed rapidly after, a disruption of normal operations. Once an official plan has been established, train your employees on this plan. An example can be found at: http://www.fema.gov/continuity-operations



Policy and Procedure—Emergency Action Plan

Options for Consideration:

Consider developing a comprehensive emergency action plan for your facility. This plan may include, but is not limited to emergency phone numbers, utility company contacts, utility operation procedures, and procedures for chemical spills, severe weather, earthquakes, bomb threats, etc. An example can be found at: www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.doc

Policy and Procedure—Evacuations and Assembly Areas

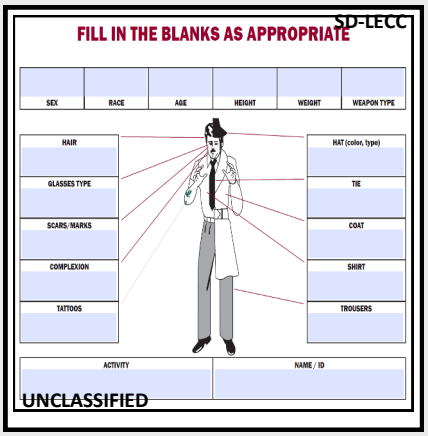
Options for Consideration:

Consider developing a comprehensive evacuation plan for your facility. This plan may include, but should not be limited to, conditions that may warrant evacuation vs. shelter in place, evacuation routes, roles/responsibilities, procedures to account for all employees/contractors, and primary/backup gathering locations. Each unique crisis may require different assembly areas: earthquake and fire emergencies may be similar, but active shooter incidents may require an alternative plan. Rehearse and review the plan as appropriate.

Policy and Procedure—Active Shooter Plan/Training

Options for Consideration:

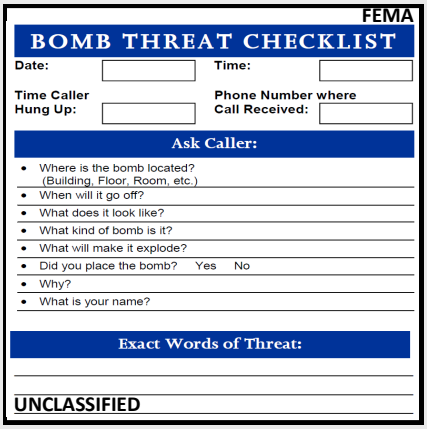
Consider developing a comprehensive active shooter plan and have employees watch the "Run, Hide, Fight" training video for basic awareness. Once an official plan has been established, train your employees on the plan. At a minimum, ensure the employees that are located at reception or near building entrances have a plan to alert others if a workplace violence incident occurs. An example can be found at: http://www.readyhoustontx.gov/videos.html



Policy and Procedure—Suspicious Activity Reporting

Options for Consideration:

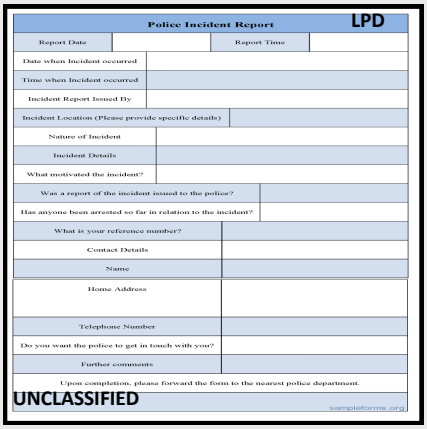
The attachment at the end of the document can assist with collecting detailed and complete information to help investigate crimes or suspicious activity. This form can be kept at a desk, in a vehicle, or any place where one can easily access it if a crime or suspicious activity is observed. Please report crimes and suspicious activity to both local law enforcement and local fusion centers. Also, consider sharing local incidents with similar facilities to ensure increased awareness.



Policy and Procedure—Bomb Threats

Options for Consideration:

Consider placing bomb threat checklists near every phone. This checklist may provide reminders of information to collect from the caller if a bomb threat is received. This information may be essential in the law enforcement investigation and potential apprehension of the responsible parties. Ensure your facility has an approved policy and procedure for what to do during and after a received bomb threat. Bomb checklist example: http://emilms.fema.gov/is906/assets/ocso-bomb_threat_samepage-brochure.pdf



Policy and Procedure—Security Log

Options for Consideration:

Consider having employees/patrols keep a daily log sheet to record safety/security information. Ensure that all employees are made aware of suspicious activities and include pictures/videos as well as a written description of incidents. This may help raise awareness to employees, and may be vital information for law enforcement to help investigate incidents involving the facility.

Policy and Procedure–Suspicious Mail

Options for Consideration:

Provide basic suspicious mail training to all individuals that may handle deliveries. A training video produced by the State of Illinois is available online at https://www.illinois.gov/ready/hazards/pages/suspiciousmail.aspx *Suspicious -Unknown-Package's* (The awareness section is from 2:45—7:00 minutes) In addition, awareness posters can be downloaded from http://about.usps.com/posters/pos84.pdf

Policy and Procedure—Communications Plan

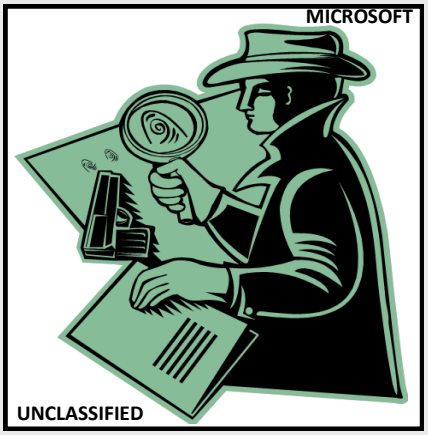
Options for Consideration:

Consider developing a plan to communicate pertinent information to employees and individuals present at your facility during a crisis. The plan should include all methods of communication to convey information to personnel such as phone trees, mass email, mass text, landline and mobile phone calls, public announcement systems, radios, etc. The communications plan should be available to all employees and rehearsed as appropriate.

Policy and Procedure—Personnel Termination Procedures

Options for Consideration:

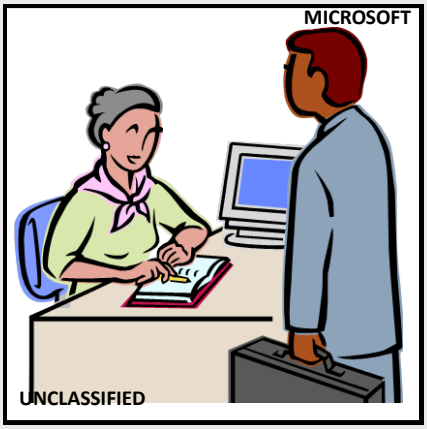
Consider having formal termination procedures in place to ensure a terminated employee is escorted off the property without incident, and that security personnel/employees are aware that the terminated employee is no longer allowed on the property. Also, consider using a checklist to ensure sensitive items, such as keys, badges, equipment, etc., are returned. This should also include disabling access to IT systems.



Policy and Procedure—Personnel Background Checks

Options for Consideration:

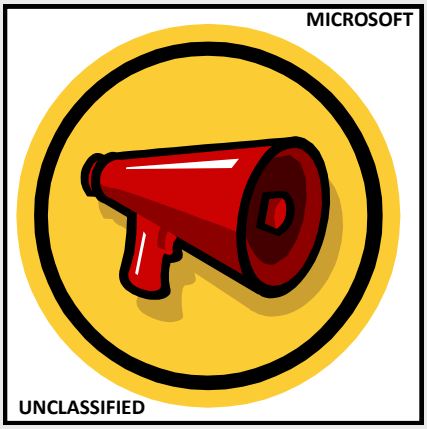
Consider conducting background checks on all employees, and applicants to prevent hiring unsuitable and potentially dangerous candidates. Ensure that contracts that cover outside vendors and contractors require the contracting company to conduct background checks on employees working at your facility.



Policy and Procedure—Visitor Access Control

Options for Consideration:

Consider having security procedures in place for visitors, to include having visitors sign a log book, verifying the visitor's ID/credentials, providing the visitor with a visitors badge, and escorting the visitor to their destination.



Policy and Procedure—Public Address (PA) System

Options for Consideration:

If a PA system is available, ensure that employees are aware of how to operate it and under what circumstances it should be used. Consider posting user instructions where the PA system is operated. Having instructions readily available may assist during a crisis and may also be helpful for new or temporary employees.

Physical Barriers/Site Hardening—Utilities—Water

Options for Consideration:

If the water line entering the facility is near the parking lot and exposed to accidental or intentional damage caused by vehicles, place appropriate barriers around the water line. To maintain aesthetics, consider using large rocks/boulders as opposed to bollards. Ensure appropriate personnel are trained in procedures to shut off the water in an emergency. Always consult the respective utility company before installing any physical security measures.

Physical Barriers/Site Hardening—Utilities—Electricity

Options for Consideration:

If the electrical transformer is near the parking lot or roadway and exposed to accidental or intentional damage caused by vehicles, place appropriate barriers around the transformer. To maintain aesthetics, consider using large rocks/boulders as opposed to bollards. Ensure appropriate personnel are trained in procedures to shut off the electricity in an emergency. Always consult the respective utility company before installing any physical security measures.

Physical Barriers/Site Hardening—Utilities—Natural Gas

Options for Consideration:

If the natural gas line entering the facility is near the parking lot and exposed to accidental or intentional damage caused by vehicles, place appropriate barriers around the natural gas line. To maintain aesthetics, consider using large rocks/boulders as opposed to bollards. Ensure appropriate personnel are trained in procedures to shut off the natural gas in an emergency. Always consult the respective utility company before installing any physical security measures.

Physical Barriers/Site Hardening—Utilities—Concealment

Options for Consideration:

For utilities that are behind chain link fencing, consider placing chain link fence privacy slats or fabric around the enclosure. This will assist in concealing critical components. This may require adding more Closed Circuit Television (CCTV) cameras for surveillance, if you have concerns regarding visibility of the components. Always consult the respective utility company before installing any physical security measures.

Access Control—Proximity Card Readers

Options for Consideration:

Consider using proximity card readers combined with a scramble key pad for controlled access to critical areas. Having a proximity card reader and a keypad means that a stolen card can not be used without the issued pin number. Use of a scrambled keypad means bystanders cannot acquire a pin by observing what keys are depressed. It also offers the ability to disable lost cards and track what individuals have accessed controlled areas.

Access Control—Employee Identification Cards/Badges

Options for Consideration:

Consider issuing employee identification badges that must be visibly worn while in the facility. This allows for quick identification of authorized and unauthorized personnel.

AVON AND SOMERSET CONSTABULARY

UNCLASSIFIED

Access Control—Security Screws

Options for Consideration:

Ensure that door latch protectors, door security plates, window security bars, ventilation grates, etc. are not screwed in with common flat or Phillips head screws. These screws can easily be removed to bypass security measures. Use security screws or "one-way" screws to ensure that security measures cannot easily be defeated.

SAN DIEGO READER

UNCLASSIFIED

Access Control—Roof Access/Window Security

Options for Consideration:

Consider doing a site security survey to check for locations in which individuals can access your facility's roof from the ground level. Consider relocating or removing objects that can assist individuals in gaining access to the roof. If this is not possible by design, consider installing alarm systems on the doors/windows that can easily be accessed from rooftop locations.

SD-LECC

UNCLASSIFIED

Access Control—Roof Access Hatch

Options for Consideration:

Consider locking or alarming roof access points to prevent unauthorized access to the interior of the building. Often these points of access are left unsecured.

Access Control—Anti-Pry Plates

Options for Consideration:

Consider adding anti-pry protection (latch guards) on doors to increase facility security and reduce the risk of an intruder using a pry bar to gain access to the facility.

Access Control—Key Control Policy

Options for Consideration:

Consider implementing a key control policy to include rules for issuing keys, deposit for keys, duplication of keys, numbering of keys, lost/stolen keys, termination/separation of employees with keys, repair of doors/locks, storage of keys, etc.

Access Control—Window Security

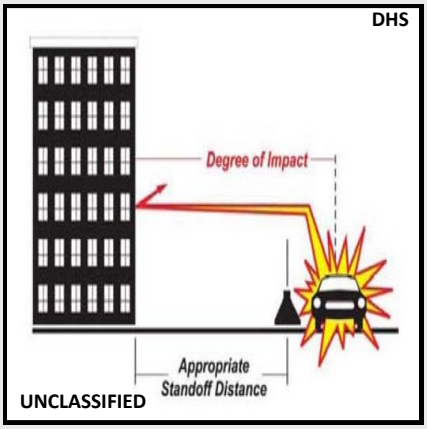
Options for Consideration:

Consider adding high security windows or retrofit all windows with aftermarket devices to increase security. Immediate low cost options include adding dowel rods or screw-in window locks on the inside track of sliding windows. Consider also adding window security film to increase shatter resistance.

Access Control—Window/Door Pins

Options for Consideration:

Ensure window and door hinge pins are secured. Consider spot welding the pins in place to prevent the pins from being removed as a method of unauthorized entry.



Access Control—Standoff Distance

Options for Consideration:

Consider extending the facility perimeter using fencing, planters, bollards, boulders, or other obstructions to vehicles to improve standoff distance and decrease destructive effects of a vehicle borne improvised explosive device.

Access Control—Vehicle Access

Options for Consideration:

Consider placing planters, bollards, boulders, or other vehicle obstructions in front of entrances of a facility to prevent accidental or intentional ramming. These may be especially important at access points with multiple doors that may allow for penetration into the building by a vehicle.

Access Control—Parking Lot

Options for Consideration:

Consider offering free non-descript parking permit stickers to patrons. Consider enforcing that no vehicles are allowed to park overnight in facility parking lots. It is easier to determine if a car is unauthorized if the parking lot has an established and consistent pattern of being empty during off hours and you can determine if the vehicle is owned by a vetted patron.

Access Control—Door Locks

Options for Consideration:

Exterior doors that have a single door knob can easily be sheared off. Consider replacing or adding door knobs with a single or double cylinder dead bolt lock. This may be a simple and cost effective way to add security to a sensitive area.

Access Control—Fence Line

Options for Consideration:

Determine if the perimeter of your fence is free from damage. Check the perimeter of your fence to determine if there are locations in which items can be used to bypass the fence. Make any necessary repairs. Remove any vegetation or manmade objects that can be used to assist a person to climbing over your fence line. i.e. dumpsters, sheds, garbage cans, ladders, patio furniture, or debris. The appearance of good security may assist deterring criminal activity.

Access Control—Front Reception

Options for Consideration:

To provide the maximum protection for the front reception area, install ballistic rated glass and equal protection for the surrounding walls. Ensure the glass does not have holes that would allow a person to stick a weapon through.

Access Control—Loading Docks

Options for Consideration:

Loading docks are often vulnerable to unauthorized access. To reduce vulnerabilities consider manning loading docks with security personnel to control access, and verify the identification documents of delivery companies/drivers. Security personnel could also inspect deliveries for suspicious indicators prior to packages entering the facility.

Detection—Stairwell Mirrors

Options for Consideration:

Consider adding security mirrors (half-dome mirrors) within the stairwells of your facility, especially the stairwells that exit outside of the building. This will add a layer of security by allowing individuals to see around corners before entering the stairwell.

Detection—CCTV/Video Processing

Options for Consideration:

Consider adding CCTV cameras to cover the entire perimeter of all critical areas. Ensure cameras work well in low light conditions. Ensure that camera cables are secured by running them through the wall or within conduit. Ensure that designated employees are trained on how to retrieve video data. Ideally, have a written process for data retrieval so that first responders can access the video in an emergency.

Detection—Motion Activated Lighting

Options for Consideration:

Consider completing a lighting survey at night. Determine areas of inadequate lighting and augment current lighting to present a clear and uniform illumination. Good lighting can serve as a deterrent for illicit activity. If a camera cannot be added, consider adding motion activated lighting in the area. The activation due to motion may provide an increase in detection and deterrence capabilities.

Detection—Suspicious Packages

Options for Consideration:

Consider making it policy that employees promptly move deliveries to the inside of an office/room if packages are delivered outside in general areas. Packages that are left sitting outside may appear as commonplace and may make it less likely that a suspicious package may be detected. Another option may be to use an offsite mailbox to limit deliveries directly to the facility.

Detection—Law Enforcement Traffic Assistance

Options for Consideration:

If traffic flow during facility events is an issue, determine if extra traffic assistance can be provided by your local law enforcement agency to help minimize accidents and/or other traffic related issues. Consider discussing with your city the possibility of painting extra cross walks and hiring or recruiting volunteers.

Detection—Height Indicator Tape

Options for Consideration:

Many businesses place measuring tape near the public access doors to assist with easily determining a person's height. This information may be helpful for law enforcement investigating an incident. At a minimum, measure items currently in place (plants, jacket hangers, etc.) so that the front desk attendants can easily determine the height of an individual using those items as a reference.

Detection—Alarm System

Options for Consideration:

Consider installing an alarm system that monitors entrances and windows for unauthorized access. Ensure alarms systems are remotely monitored 24/7 and can notify local law enforcement and facility personnel in the event of unauthorized entry. Ensure the alarm system control panel is not located near a window in which the status of the alarm or alarm codes could be observed by unauthorized individuals.

Detection—Security

Options for Consideration:

Consider hiring private security personnel to maintain situational awareness at a facility. Presence of security personnel, armed or unarmed, may act as an effective deterrence against attacks. When taking this into consideration, an attacker may choose to select a "softer" target without security personnel rather than a facility with security personnel.

Detection—Confidential Reporting System

Options for Consideration:

Consider developing a confidential reporting system to allow employees to provide information on suspicious behavior/activities within the facility. In many incidents of workplace violence, at least one person had prior knowledge of the attacker's intent, potential indicators, or observed suspicious behavior before the incident took place. This system can provide actionable information that could thwart a violent incident.

Emergency Preparedness— Fire Suppression Control

Options for Consideration:

If you have a waterless fire suppression system, consider training all employees on how this system works, including the abort function. If there is a situation where the abort function must be activated, this system typically requires a person to hold the button until the system is reset. This may require holding the button until the fire department or other trained personnel arrive to perform the reset.

Emergency Preparedness—Emergency Lighting

Options for Consideration:

Consider purchasing flashlights and strategically placing them throughout the office in the event of loss of electricity. Ensure that all employees are aware of the location of emergency flashlights. Ensure that flashlights are in working order and have additional batteries available or are rechargeable plug in flashlights.

Emergency Preparedness—Automated External Defibrillator (AED)

Options for Consideration:

If your facility is equipped with an AED or Trauma Kit, ensure that all employees are aware of what equipment is available and where it is located. Consider hosting training on the use of the equipment.

Other—Maintenance

Options for Consideration:

Consider doing a facility wide assessment of the perimeter, outside spaces, and all interior rooms to remove, discard, and organize excess materials. Ensure broken fence lines, lights, posts, signs, etc. are quickly repaired. A well maintained facility gives the appearance of a well managed facility and may provide as a deterrence to criminal activity.

Terms and Definitions

Access Control– the control of persons, vehicles, and materials through the implementation of security measures for a protected area.

Asset– any tangible or intangible value (people, property, information) to the organization.

Barrier– a natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials.

Business Continuation Planning-the process of analyzing an organization's business to determine the impact of a loss or disruption of service.

Closed-Circuit Television (CCTV)- video surveillance system; a television installation in which a signal is transmitted to monitors, recorders and control equipment.

Continuity of Operations Plan (COOP)– series of plans used to respond, recover, resume and restore from a business interruption.

Detection– the act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter.

Emergency Action Plan– a plan of action to commence at the time of an incident to prevent the loss of life and minimize injury and property damage.

Intrusion Detection System (IDS)- a security alarm system consisting of various types of components (balanced magnetic switches, capacitance, infrared, ultrasonic, etc.) to detect intrusion in the area of coverage within a facility.

Physical Security– security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, materials, and document, and to safeguard them against a security incident.

Physical Security Measure– a device, system, or practice of a tangible nature designed to protect people and prevent damage to, loss of, or unauthorized access to assets.

Policy– a leadership statement that indicates the direction or intent of an organizational propose for a given subject area.

Procedure– detailed implementation instructions for carrying out policies; often presented as forms or list of steps to be taken prior to, during and following an incident.

Security Manager– an individual with management-level responsibility for the security program of a organization or facility.

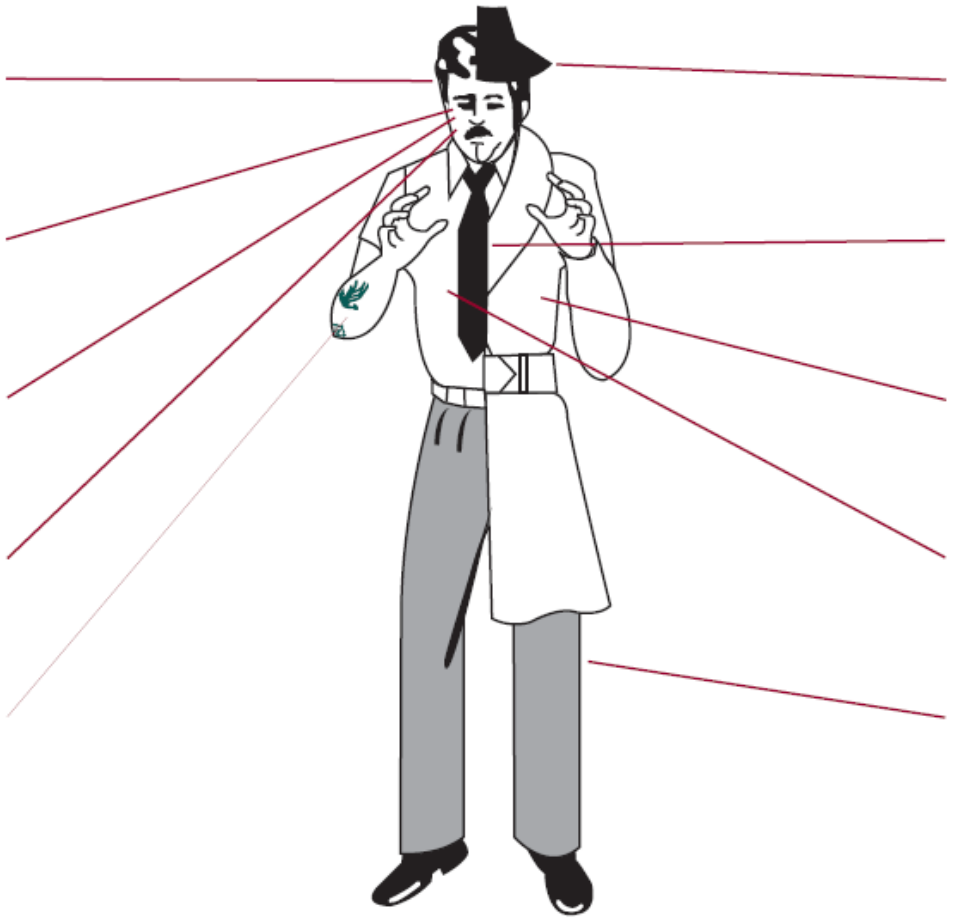
Security Vulnerability– an exploitable security weakness.

Site Hardening– implementation of enhancement to make a site more difficult to penetrate.

Threat– an action or event that could result in a loss or an indication that such an action or event may take place.

FILL IN THE BLANKS AS APPROPRIATE

SEX	RACE	AGE	HEIGHT	WEIGHT	WEAPON TYPE

HAIR		HAT (color, type)
GLASSES TYPE		TIE
SCARS/MARKS		COAT
COMPLEXION		SHIRT
TATTOOS		TROUSERS

ACTIVITY	NAME / ID

FILL IN THE BLANKS AS APPROPRIATE

ACTIVITY		DIRECTION OF ESCAPE	
PLATE	**MAKE/MODEL**	**COLOR**	**GRAPHICS**
WHEELS	**WINDOWS**	**LIFTED/LOWERED**	**MISC.**