



## **SECURITY ALERT**

*Physical Security*

### **OFFICE SECURITY**

Government offices can be targets for theft, unlawful entry, kidnapping, bombings, forcible occupation, and sabotage. Effective barriers, both physical and psychological can reduce the likelihood of these threats. The following guidelines will help you analyze your office security profile and suggest measures to reduce your target potential.

**Conduct a Crime Prevention Assessment** - A complete, professional assessment of your security needs is the first step toward an effective security program. Your nearest Federal Protective Service (FPS) office can arrange a risk assessment be performed on your government-owned or leased office or building.

Since most crimes are directed toward individuals or offices that have little or no security planning in place. Take stock of your present measures and possible weak points. A comprehensive crime prevention assessment should ask:

- What is your target potential?
- What is the prevailing attitude toward security?
- Who is responsible for the overall security program?
- How are security policies enforced?
- When was the current emergency preparedness plan developed (including fire, power failure and disaster)?
- What resources are available locally and how rapid are the response times for fire, police, and ambulance?
- What kind of physical security systems and controls are presently used?
- Do the available security resources, policies and procedures meet the potential threat?

**Take Reasonable Precautions** - Once the risk assessment has been completed, follow up with the FPS (or local law enforcement group) to act on the findings. For example, publicize phone numbers and make sure everyone knows whom to contact in case of an emergency.

#### **General suggestions that may increase your security:**

- Install key-card access systems at main entrances and on other appropriate doors.
- Issue access control badges, with recent photographs, to all employees and authorized contractors.
- Upgrade perimeter control systems with intercoms and closed-circuit monitoring devices.
- Keep master and extra keys locked in a security office.
- Develop crisis communication among key personnel and security office involving intercoms, telephones, duress alarms or other concealed communications.
- Have a backup communication system, like two-way radio, in case of phone failure.
- Locate executive offices near the inner core of the building to afford maximum protection and avoid surveillance from the outside.
- Arrange office space so unescorted visitors can be easily noticed.
- Have staff follow strict access control procedures, don't allow exceptions.
- Keep important papers locked in secure cabinets.

Gemini Tech Services, LLC

5019 E. I-20, Frontage Rd, Willow Park, TX 76087 / (T) 682-708-8581 / [www.geminitechservices.com](http://www.geminitechservices.com)

Small Business Administration Certified 8(a) and Economically Disadvantaged – Woman Owned /Minority Owned Small Business



- Keep offices neat and orderly to identify strange objects or unauthorized people more easily.
- Empty trash receptacles often.
- Open packages and large envelopes in executive offices only if the source or sender is positively identified.
- Keep closets, service openings, telephone and electrical closets locked at all times. Protect crucial communications equipment and utility areas with an alarm system.
- Avoid stairwells and other isolated areas. Try not to ride the elevator alone with a suspicious person.
- Do not work late alone or on a routine basis.
- Keep publicly accessible restroom doors locked and set up a key control system. If there is a combination lock, only office personnel should open the lock for visitors.

## **PHYSICAL SECURITY IN A FRONT-LINE OFFICE**

If your office is a Federal "front-line" office with direct "employee-to-customer" service, your office and building should be designed according to Federal Protective Service security guidelines. If the agency you provide services for does not have security procedures in place, the head of the agency you support may want to ask a regional GSA Federal Protective Service office to conduct a physical security survey to ensure that employees are working in a safe and secure environment.

Before requesting a security survey, the agency may want to do a "crime assessment" of the risks you and your coworkers may encounter in your workplace. Are your customers likely to experience elevated levels of stress or tension? Do members of the general public who come into the office tend to be argumentative? Have there been threats or incidents of violence involving the public in the past? Or have Federal and Contractor employees themselves become violent or threatening?

If your front-line public service office fits this profile, the agency should take immediate steps to help make your workplace become fully secure. Following are some suggestions on improving security in your office and/or building.

- Post a security guard at the main building entrance or at entrances to specific offices. Officers (or guards) should have a clear view of the controlled area at all times.
- Install a metal detector or CCTV (closed-circuit television) camera or other device to monitor people coming in all building entrances.
- Issue all employees photo identification cards and assign temporary passes to visitors--who should be required to sign in and out of the building. Under certain conditions, FPS officers (or contract guards) should be required to call Federal offices to confirm an appointment and/or to request an escort for all visitors--customers, relatives, or friends.
- Rearrange office furniture and partitions so that front-line employees in daily contact with the public are surrounded by "natural" barriers--desks, countertops, partitions--to separate employees from customers and visitors.
- Brief employees on steps to take if a threatening or violent incident occurs.
- Establish code words to alert coworkers and supervisors that immediate help is needed.
- Provide an under-the-counter duress alarm system to signal a supervisor or security officer if a customer becomes threatening or violent.
- Establish an area in the office for employees and/or customers to escape to if they are confronted with violent or threatening people.

### **Physical Security Features in a Customer Service Federal Office**

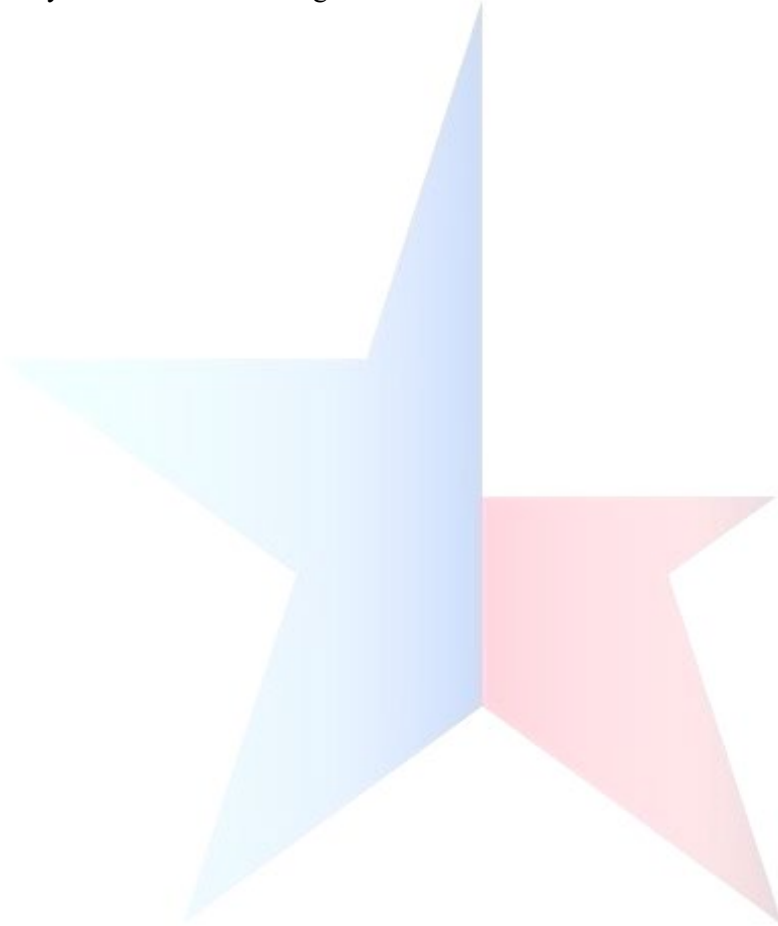
**Gemini Tech Services, LLC**

5019 E. I-20, Frontage Rd, Willow Park, TX 76087 / (T) 682-708-8581 / [www.geminitechservices.com](http://www.geminitechservices.com)

Small Business Administration Certified 8(a) and Economically Disadvantaged – Woman Owned /Minority Owned Small Business



- Single public entrance to customer service area.
- Reception desk immediately inside public entrance.
- Silent, concealed alarms at reception desk and on Federal employee side of service counter.
- Barrier between customer waiting and Federal work areas.
- Service counter with windows between Federal employees and customers.
- Window in supervisor's office from which supervisor can view customer service.
- Access-control combination locks on access doors
- Closed circuit television camera mounted for monitoring customer service activity from a central security office for the building.



**Gemini Tech Services, LLC**

5019 E. I-20, Frontage Rd, Willow Park, TX 76087 / (T) 682-708-8581 / [www.geminitechservices.com](http://www.geminitechservices.com)  
Small Business Administration Certified 8(a) and Economically Disadvantaged – Woman Owned /Minority Owned Small Business