Security Vulnerability Assessment

Guide for Critical Infrastructure Protection

Courtesy of:

DATE: _____, 20____

Important Note:

This document contains sensitive information about the security of your infrastructure. Therefore, it should be treated as Confidential Information and should be stored in a secure place in the organization. A duplicate copy should also be stored in a secure off-site location.

Keep this Document

This is a working document. Its purpose is to start your process of security vulnerability assessment and security enhancements. Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade.

Don't forget that this is a sensitive document. It should be stored separately in a secure place at your organization. A duplicate copy should also be retained at a secure off-site location. Access to this document should be limited to personnel, state and local officials, and others on a need-to-know basis

Disclaimer:

This Security Vulnerability Assessment is designed to help you determine possible vulnerable components and identify security measures that should be considered. A "vulnerability assessment" is the identification of weaknesses in infrastructure security, focusing on defined threats that could compromise its ability to provide adequate services. This document is meant to encourage you to review your infrastructure vulnerabilities, but it does not take the place of a comprehensive review conducted by security experts. This assessment was designed to provide baseline recommendations and actions you should take to improve security

Introduction

Infrastructures are critical to every community. Protection of those infrastructures must be a high priority to ensure uninterrupted service and safety, which is essential for the protection of public safety.

Adequate security measures will help prevent loss of service through vandalism, burglary, pranks, fire and acts of terror. If your infrastructure is prepared, such actions may even be prevented. The appropriate level of security is best determined at the local level.

This Security Vulnerability Assessment is designed to help you determine possible vulnerable components and identify security measures that should be considered. A "vulnerability assessment" is the identification of weaknesses in infrastructure security, focusing on defined threats that could compromise its ability to provide adequate services.

This document is meant to encourage you to review your infrastructure vulnerabilities, but it may not take the place of a comprehensive review by security experts. The Assessment was developed with a simple design with recommendations we provide to assist you to improve the security of your facility.

This document is to be used by personnel within the organization. Physical facilities pose a high degree of exposure to any security threat.

The Assessment includes an emergency contact list for your use. This list will help you identify who you need to contact in the event of an emergency or threat and will help you develop communication and outreach procedures. Filling out the Emergency Contact List is an important step toward developing an Emergency Response Plan, which provides detailed procedures on how to respond to an emergency. You may obtain sample Emergency Response Plans from the Division of Homeland Security.

Record of Security Vulnerability Ongoing Assessment

Name	
Title	
Area of Responsibility:	
Company/Infrastructure:	
Address	
City	
County	
State	
Zip Code	
Telephone	
Fax	
E-mail	
Date Completed	

Record of Security Vulnerability Ongoing Assessment [Record of Revisions]

Date Revised	Name	Signature

Executive Summary

Security Vulnerability Assessment

This executive summary outlines the business' primary mission and the critical assets or components to support providing a safe and secure environment.

Business Name	
Business Address	
City, State, Zip Code	
County	
Primary Mission:	

Critical Assets or Components	**Function**

Emergency Contact Information:

Identify three (3) independent departments within your business for emergency contact.

Name and Title or Department	Office Number	Mobile Number	Email

Security Vulnerability Assessment

Section 1: General Questions for the Facility			
The first 13 questions in this vulnerability assessment are general questions designed to apply to all components of your facility (buildings, equipment, storage areas, and equipment storage sites). These are followed by more specific questions that look at individual components in greater detail.			
QUESTION	**ANSWER**	**RECOMMENDATIONS**	**ACTION NEEDED**
1. Does organization have a written emergency response plan (ERP)?	Yes ☐ No ☐	It is essential that your organization have an ERP. If you do not have an ERP, you can obtain a template from our website. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2). A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies. You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to your security provider, local police department, emergency personnel and local officials (if applicable). Share this ERP with police, fire department, emergency personnel and designated staff.	

2. Is access to the critical components of the facility (i.e., a part of the physical infrastructure of the facility that is essential for sensitive operations) restricted to authorized personnel only?	Yes ☐ No ☐	You should restrict or limit access to the critical components of your facility to authorized personnel only. This is the first step in security enhancement for your infrastructure. Consider the following: ▪ Issue company photo identification cards for employees (where appropriate) and require them to be displayed within the restricted area at all times. ▪ Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID. ▪ Treat the information herein as sensitive and highly confidential, which could pose a security risk if posted for public viewing as it provides information that could be used against the facility.	
3. Are facilities fenced and are gates locked where appropriate?	Yes ☐ No ☐	Ideally, all facilities should have a security fence around the perimeter. The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.	

4. Are doors, windows, and other points of entry such as roof hatches and vents kept closed and locked?	Yes ☐ No ☐	Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost. A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place. Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside. If unable to locate hinges on the inside of the building have the hinges been welded to prevent entry. Ensure all security enhancements meet fire code requirements. Alarms can also be installed on windows, doors, and other points of entry.	
5. Does facility have external lighting around critical components?	Yes ☐ No ☐	Adequate lighting of the exterior of the facility's critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that activate switches that turn lights on or trigger alarms also enhance security.	

6. Are warning signs (no trespassing, no unauthorized access, etc.) posted on all critical components of facility?	Yes ☐ No ☐	Warning signs are an effective means to deter unauthorized access. "Warning - Tampering with this facility is a federal offense" "No Trespassing," "Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.	
7. Does security patrol and inspect buildings, equipment, equipment storage sites, and other critical components?	Yes ☐ No ☐	Frequent and random patrolling your facilities staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol. Ensure your security provider conducts frequent patrols of your facilities. Advise them of your critical components and explain why they are important.	
8. Is the area around the critical components of facility free of objects that may be used for breaking and entering?	Yes ☐ No ☐	When assessing the area around your facility's critical components, look for objects that could be used to gain entry (e.g., vehicles, equipment, large rocks, cement blocks, pieces of wood, ladders, and other tools)	

9. Are the entry points to the facility easily seen?	Yes ☐ No ☐	You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities. Trim trees and shrubs to enhance the visibility of your facility's critical components. If possible, park vehicles and equipment in places where they do not block the view of your critical components.	
10. Is there an alarm system that will detect unauthorized entry or attempted entry at critical components?	Yes ☐ No ☐	Consider installing an alarm system that notifies the proper authorities or your facility's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available and should be considered whenever possible for securing sensitive items. You should also have an audible alarm at the site as a deterrent and to notify employees and/or tenants of a potential threat.	
11. Does the organization have a key control and accountability policy?	Yes ☐ No ☐	Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use. Keep the key to the key box secure location not in the top drawer next to the key box.	

12. Are entry codes and keys limited to company personnel only?	Yes ☐ No ☐	Suppliers and personnel from co-located organizations (e.g., organizations using your facility for telecommunications) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of company personnel.	
13. Does facility have a neighborhood watch program?	Yes ☐ No ☐	Watchful neighbors can be very helpful to a security program. Make sure they know whom to call in the event of an emergency or suspicious activity.	

Section 2: Suppliers			
Facilities should **not** provide easy access for suppliers of equipment, chemicals, and other materials for the convenience of both parties.			
QUESTION	**ANSWER**	**RECOMMENDATIONS**	**ACTION**
14.Are deliveries of chemicals and other supplies made in the presence of company personnel?	Yes ☐ No ☐	Establish a policy that an authorized person, designated by the facility, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the facility.	
15.Has organization discussed procedures with supplier(s) to ensure the security of their products?	Yes ☐ No ☐	Verify that your suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your facility. You should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo I.D.), date, time, material delivered, and the supplier's name.	

16. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?	Yes ☐ No ☐	All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. You should have tools and equipment on site (such as a fire extinguisher, dry sweep, etc.) to take immediate actions when responding to an emergency.	

Section 3: Personnel			
Your organization should add security procedures to your personnel policies			
QUESTION	**ANSWER**	**RECOMMENDATIONS**	**ACTION**
17. When hiring personnel, does organization perform a criminal background check and verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?	Yes ☐ No ☐	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues. If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	
18. Are personnel issued photo-identification cards?	Yes ☐ No ☐	For positive identification, all personnel should be issued company photo-identification cards and be required to display them at all times. Photo identification will also facilitate identification of authorized company personnel in the event of an emergency.	
19. When terminating an employee, is employee required to turn in photo IDs, keys, access codes, and other security-related items?	Yes ☐ No ☐	Former or disgruntled employees have knowledge about the operation of your company, and could have both the intent and physical capability to harm your facility. Requiring employees who will no longer be working at your company to turn in their IDs, keys, and access codes helps limit these types of security breaches.	

20. Do employees (where appropriate) wear uniforms with company/ organization name prominently displayed?	Yes ☐ No ☐	Requiring appropriate personnel to wear uniforms and requiring vehicles to prominently display company name helps inform the public when your staff is working. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to security or law enforcement authorities.	
21. Have company personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes ☐ No ☐	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity. Periodic meetings of authorized personnel should be held to discuss security issues.	
22. Do personnel and security provider have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes ☐ No ☐	To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to security provider and appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included in Attachment 3. Also make sure caller ID is activated on your telephone system to keep a record of incoming calls.	

Section 4: Information storage/computers/maps			
Security of your facility includes information storage, computers, facility maps goes beyond the physical aspects of your company. It also includes records and critical information that could be used by someone planning to disrupt or destroy your facility			
QUESTION	**ANSWER**	**RECOMMENDATIONS**	**ACTION**
23. Is computer access "password protected" with secure passwords that are difficult to compromise? Is virus protection installed and software upgraded regularly and are virus definitions updated at least daily? Is Internet firewall software installed on all computers and data regularly backed up?	Yes ☐ No ☐	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. Each individual should have a unique password that is not shared. Passwords should be at least eight characters long, not contain the user name, real name, company name or a complete word; and also contain at least one character from each of the following categories: ▪ Uppercase letters ▪ Lower case letters ▪ Numbers ▪ Symbols. Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Your organization should protect sensitive data by routinely making backup copies of computer data stored at a secure off-site location and subscribing to a virus protection program.	

24. Is there information on the Web that can be used to disrupt facility?	Yes ☐ No ☐	Posting detailed information about your facility on a Web site may make your facility more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed. Perform a Web search (using a search engine such as Google, Yahoo!, or Bing) using key words related to your facility to find any published data on the Web that is easily accessible by someone who may want to damage your facility.	
25. Are maps, records, and other information stored in a secure location?	Yes ☐ No ☐	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only. You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	
26. Are copies of records, maps and other sensitive information labeled confidential, and are all copies controlled and returned to company?	Yes ☐ No ☐	Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.	

27. Are vehicles locked and secured at all times?	Yes ☐ No ☐	Vehicles are essential to any company. They typically contain maps and other information about the operation of the facility. Company personnel should exercise caution to ensure that this information is secure. Company vehicles should be locked when they are not in use or left unattended. Remove any critical information about the company before parking vehicles for the night. Vehicles also usually contain tools that could be used to access your facility and are costly to replace. These tools should be secured and accounted for daily.	

Section 5: Public Relations			
You should educate your customers and/or about your facility. You should encourage them to be alert and to report any suspicious activity to security and/or law enforcement authorities			
QUESTION	**ANSWER**	**RECOMMENDATIONS**	**ACTION**
28. Is there a program in place to educate and encourage the public, customers or tenants to be vigilant and report suspicious activity to assist in organization's security protection?	Yes ☐ No ☐	Advise your customers and the public that your company has increased preventive security measures to protect and secure the facility. Ask for their help. Provide your telephone number and the telephone number of your security provider and local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards and flyers.	
29. Does facility have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes ☐ No ☐	You should have a procedure for personnel to follow when you receive an inquiry about the facility or its operation from the press, customers, or the general public. Your personnel should be advised not to speak to the media on behalf of the company. Only one person should be designated as the spokesperson for the company. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	

30. Does facility have a procedure in place to receive notification of a suspected threat to the infrastructure?	Yes ☐ No ☐	It is critical to be able to receive information about suspected threats within your infrastructure at any time and respond to them quickly. Procedures should be developed in advance with your local, state, and federal agencies.	
31. I s there a procedure in place to respond immediately to customer complaints?	Yes ☐ No ☐	It is critical to be able to respond to and quickly identify potential problems with customers. Procedures should be developed in advance to investigate and identify the complaint.	

Now that you have a "Security Vulnerability Assessment," review your needed actions and then prioritize them based on the most likely threats. A Table to assist you in prioritizing actions is provided in Attachment 1.

Attachment 1. Prioritization of Needed Actions

Once you have reviewed the "Security Vulnerability Assessment", review the actions you need to take to improve your facility's security. Note the questions that were answered "no" on this worksheet. You can use it to summarize the areas where your facility has vulnerability concerns. It can also help you prioritize the actions you should take to protect your facility from vulnerabilities. Make sure to prioritize your actions based on the most likely threats to your facility**.**

Question #	Corrective Action	Due Date

Question #	Corrective Action	Due Date

Attachment 2. Emergency Contact List

We urge all critical infrastructures to adopt an emergency response plan (ERP). Emergency response plans are action steps to follow if the infrastructure is compromised or if the service is disrupted. You can obtain an ERP template from our website.

The "Emergency Contact List" is an essential part of your ERP. It contains the names and telephone numbers of people you might need to call in the event of an emergency. This is a critical document to have at your disposal at all times. It gives you a quick reference to all names and telephone numbers that you need for support in the case of an emergency.

Filling out this Emergency Contact List reminds you to think about all of the people you might need to contact in an emergency while encouraging you to communicate with key people.

Section 1. Company/Infrastructure Information		
Company/Infrastructure Name		
Company/Infrastructure Address		
City, State, Zip Code		
Telephone Numbers	Main	Evening/Weekend
Other Contact Numbers	Main Fax	Email
Population Served and Number of Service Connections	People Served	Connections

Name, title, and telephone number of person responsible for company/infrastructure security	Name and Title	Home Number
		Office Number
	Email	Cellular Number
		Pager Number
Name, title, and telephone number of person responsible for maintaining emergency contact list	Name and Title	Home Number
		Office Number
	Email	Cellular Number
		Pager Number

Section 2. Notification / Contact Information

Local Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE (DAY)	EMAIL
Homeland Sec. Field Office			
Highway Patrol			
Police Department			
Sheriff's Office			
FBI Field Office			
Fire Department			
Local HAZMAT Team			
EMS			
Federal Regulating Department			
State Regulating Department			
Local Government Official			
Local Emergency Manager			
Local Emergency Planning Committee			
Local Hospital			
Local Schools			
Neighborhood Watch Program			

Service / Repair Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE	EMAIL
Security / Alarm Company			
Electric Utility Company			
Gas Utility Company			
Sewer Utility Company			
Telephone Utility Company			
Computer Specialist			
Construction Contractor			
Electrical Contractor			
Plumbing Contactor			
Local Disaster Cleanup			
Blue Stakes			
Equipment Rental			

Section 3. Communication and Outreach Communication

Communications during an emergency can create special problems. A standard response in an emergency is to call "911" for local fire and police departments. But what if the emergency has disrupted telephone lines and over-loaded cell phone lines? Talk with the Division of Homeland Security and your state-regulating department about local emergency preparedness and solutions to these problems. Increasingly, state emergency agencies are establishing secure lines of communication with limited access. Learn how you can access those lines of communication if all others fail.

Outreach

If there is an incident that the infrastructure is compromised or if the service is disrupted, you will need to notify Emergency Services and make recommendations for continuity of service. To do this, you need a plan.

How will you reach all customers, employees or tenants within the first 24 hours of an emergency?

Make sure to appoint a media spokesperson—a single person designated who will be authorized to make all public statements to the media.

Make arrangements for contacting institutions with large numbers of people that may be adversely affected by the disruption.

State Notification List

ORGANIZATION	CONTACT NAME /	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
State Division of Homeland Security				
National Guard				
Department of Commerce				
Department of Environmental Quality				
Department of Health				
Department of Natural Resources				

Media Notification List

ORGANIZATION	CONTACT NAME /	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Designated Media Spokesperson				
Newspaper – Local				
Newspaper				
Radio				
Radio				
Radio				

Television				
Television				
Television				

Attachment 3: Threat Identification Checklists

Telephone Threat Identification Checklist

In the event that the infrastructure receives a threatening phone call, remain calm and try to keep the caller on the line. Use the following checklist to collect as much detail as possible about the nature of the threat and the description of the caller. The bomb threat identification checklist can also be used for other potential threats. (See FBI Bomb Card)

QUESTIONS TO ASK	EXACT WORDING OF THE THREAT
1. When is the bomb going to explode?	
2. Where is it right now?	
3. What does it look like?	
4. What kind of a bomb is it?	
5. What will cause it to explode?	
6. Did you place the bomb?	
7. Why?	
8. What is your address?	
9. What is your name?	

Note if (and how) the caller seems familiar with the building by description of bomb location.

Fill out completely, immediately following the bomb threat. Check all that apply.			
CALLER'S VOICE			
☐ Calm	☐ Laughing	☐ Lisp	☐ Disguised
☐ Angry	☐ Crying	☐ Raspy	☐ Whispered
☐ Excited	☐ Normal	☐ Deep	☐ Cracking Voice
☐ Slow	☐ Distinct	☐ Ragged	☐ Accent | Nationality?
☐ Rapid	☐ Slurred	☐ Clearing Throat	☐ Familiar If YES, what did it sound like?
☐ Soft	☐ Nasal	☐ Deep Breathing	
☐ Intoxicated	☐ Loud	☐Stutter	
THREAT LANGUAGE			
☐ Well Spoken (Educated)	☐ Foul	☐ Irrational	☐ Incoherent
☐ Taped	☐ Message read by threat marker		
BACKGROUND SOUNDS			
☐ Street Noises			
☐ Voices (Adults/Children)			
☐ Animal Noises			
☐ Music			
☐ House Noises			
☐ Office Noises			
☐ Machinery (Office/Factory)			
☐ Motors			
☐ Other			

Call Received By		Date		Time	
Telephone Number		Position		Department	
Call Reported To		Date		Time	

Report of Suspicious Activity Checklist

In the event personnel from your infrastructure or neighbors observe suspicious activity, use the following checklist to collect as much detail about the nature of the activity.

1. Types of Suspicious Activity	
☐ Breach of Security (e.g. lock cut, door forced open)	☐ Person Taking Pictures
☐ Unauthorized personnel on property	☐ Unusual Information Requests
☐ Presence of personnel at location at unusual hours	☐ Suspicion of Surveillance
☐ Breach of Security (e.g. lock cut, door forced open)	☐ Person Taking Pictures
☐ Other: (Explain)	

2. Location of Suspicious Activity:			
☐ Office	☐ Plant	☐ Equipment Yard	☐ Warehouse
☐ Construction Site		☐ Off Site Location	
☐ Other: (Explain)			

3. Description of Events:	
What made the activity suspicious?	
Breach of security (Specify nature and location)	
What made the person suspicious?	
What made the vehicle suspicious?	

4. Description of Person:					
Name		Sex		Age	
Address					
Telephone		DL Number		Ethnicity	
Height		Weight		Hair Color	
Distinguishing Marks		Clothes		Facial Hair	

5. Vehicle Information:					
Make		Model		Type	
License Plate		State		Color	
Number of Passengers		Year			
Distinguishing Marks (e.g. dents, stickers)					

6. Report Prepared By (Name, Department, and Telephone Number):			
Date of Incident		Time of Incident:	

7. Incident Reported to		Date/Time:	

8. Action(s) Taken Following Receipt of the Report:

How to Evaluate Your Current or Proposed Security Services Provider

Private security is a huge, rapidly growing, global industry that unfortunately is also plagued by lack of minimum standards, poor training and turnover that rivals the fast-food industry. The highly competitive nature of the business has unfortunately created pricing pressures and "razor- thin" margins that compel many security providers to sacrifice quality in an effort to be the “lowest cost provider” in order to “win the bid”. The unfortunate consequence is that the public is put at risk when under-trained, often inexperienced, and poorly compensated security officers are expected to be our first line of defense against security threats.

Therefore, it is imperative that when you evaluate a security provider, price should only be one consideration among many factors determining which provider will most closely align with your organization’s security needs. After all, the security of your employees, customers and/or tenants is at stake. Selecting a security provider solely on price can be a perilous mistake. One serious security breach or misstep could not only be costly, but also potentially perilous.

We’ve provided the following guide to assist you in selecting a provider that will best meet your organization’s security objectives, and most importantly keep your organization and others safe.

The following considerations should be made:

Section 1: Organizational Alignment

Your security provider is a reflection of your company; therefore it's critical that you select a provider that represents your organization with integrity and professionalism.

QUESTION	ANSWER	COMMENTS
1. Does your security provider or proposed provider maintain standards that align with your mission, culture and priorities?	Yes ☐ No ☐	
2. Do they project a level of professionalism that best represents your organization?	Yes ☐ No ☐	
3. Is your security provider or proposed provider active in relevant local and national business organizations?	Yes ☐ No ☐	
4. Do they view their role as "policing" your facility or providing a "community service"? What is your expectation of their role?	Policing ☐ Com Service ☐ Both ☐	

Section 2: Quality of Security Officers & Employee Retention

High employee turnover is a red flag and an indication of a potentially undesirable work environment. Likewise, security providers with high employee turnover (with a churn and burn attitude) are unlikely to employ quality Security Officers, therefore it's imperative your security provider treat their employees fairly and have an employee retention plan in place.

.

QUESTION	ANSWER	COMMENTS
Retention		
5. Does your security services provider or proposed provider have an employee retention plan? What does the plan entail?	Yes ☐No ☐	
6. Do they project a level of professionalism that best represents your organization?	Yes ☐No ☐	
7. Do they provide meaningful employee benefits?	Yes ☐No ☐	
8. Do they provide an environment that cultivates continuous learning and advancement?	Yes ☐No ☐	
9. Does your security provider pay its security officers a fair and competitive wage?	Yes ☐No ☐	
10. What is your security provider or proposed provider's employee retention rate? (The national turnover average for security officers is 200% per year. A high quality security services provider will experience turnover rates in the 50 to 60% range).	_____%	

Recruitment		
11. How does your security provider or proposed provider recruit security officers?		
12. What is their screening process for new security officers?		
Training & Professional Development		
13. What training does your security provider or proposed provider require?		
14. What is their commitment to ongoing training?		
15. Is there a focus on professional development of all personnel? How accessible is the training to field personnel?	Yes ☐ No ☐	
16. Do they promote from within the organization?	Yes ☐ No ☐	
17. Does the security provider offer training programs that reflect market-specific requirements and/or compliance with governmental regulations?	Yes ☐ No ☐	

Section 3: Accountability & Transparency

A reputable security services company will exceed expectations when it comes to providing accountability and transparency. Unfortunately, many companies lack process and procedure to ensure total transparency. Ask the following questions to ensure your provider meets baseline standards.

QUESTION	ANSWER	COMMENTS
18. Does your security provider or proposed provider furnish sufficient reporting capabilities that are relevant and include objective performance metrics to ensure total transparency and accountability?	Yes ☐ No ☐	
19. Are they committed to being a continuous improvement partner or do they view themselves as just another vendor?	Yes ☐ No ☐	
20. Does your security provider or proposed provider conduct (at minimum) an annual Security Vulnerability Assessment?	Yes ☐ No ☐	
21. Does your security services company provide a single, local point of contact that is responsible and accountable to you?	Yes ☐ No ☐	
22. Are there off-hours management inspections of sites?	Yes ☐ No ☐	
23. Do they provide regular reviews to ensure they are meeting milestones and to make adjustments where necessary?	Yes ☐ No ☐	

24. What technologies or process does the security provider have in place to ensure security officers are accountable and attentive to the needs of your organization (i.e. real-time reporting software)?	
25. What processes do they have in place to ensure timely communication?	
26. What is their process for incident escalation?	
27. How do they ensure consistency in staffing, support, training, communication and coordination of on-site events?	

Final Considerations

Keep in mind that a successful relationship with a security provider is based on trust, communication and alignment of goals. It is a relationship that both parties view as a partnership rather than a client/vendor relationship. Your clients, tenants and others view your security provider an extension of your organization, therefore, it is critical that you work with a provider that is a true partner and best represents your organization.

Step 1: Identify Stakeholders - Who all will be involved in the retention of your current security provider or selection of a new provider? Participants may include representatives from executive management, building management, purchasing, maintenance, etc.

Step 2: Identify Areas in Need of Improvement - Review your current program to identify problem areas or areas that need to greater attention.

Step 3: Prioritize Your Objectives - Once you've identified areas that need to be improve, prioritize which areas are most critical and work with your security provider to put together an implementation plan.

Step 4: Ask the "Experts" - Now that you've identified your objectives, uncovered areas for improvement and prioritized your objectives, ask your security provider or proposed provider to make recommendations. A quality provider will be able to present a variety of recommendations to help you meet your objectives. This is an effective test to determine if the provider can meet your needs and has your best interest in mind.

Step 5: Ensure Security Provider has Appropriate Experience - Every property, facility or organization is unique. It's important that not only your security provider have sufficient experience, but that they also have the expertise in areas that are most important to you. For example, if you regularly host events, it is important that your security provider has significant experience providing security for events. Likewise, if your security provider will be interfacing with professionals, it is important that your security officers communicate in a manner that appears as educated and articulate.

Step 6: Create a Win-Win Relationship – Whether you decide to stay with your current provider or select a new provider, it is important you meet with them to review your contract, plans, objectives and processes. Ensure that all parties are on the same page and that expectations are clearly communicated. Establish a formal process to regularly review your security program.