PRIVATE SECURITY:

Window Dressing or Real Protection? A Roadmap for Securing Sacred Spaces

APRIL 2022

Participating Partners

Combined Jewish Philanthropies — Boston

Jewish Federation of Cleveland

Jewish Federation of Greater Phoenix

Jewish Federation of Greater Pittsburgh

Jewish Federation of Greater Washington

GATEWAY GROUP ONE

Secure Community Network

JENSEN HUGHES
Advancing the Science of Safety

EXECUTIVE SUMMARY

Does hiring a private security firm make Jews safer?

Amid the rising threat of antisemitism, as well as other acts of targeted violence and hate, Jewish communities and other faith-based organizations across North America are making significant investments in professionally managed, comprehensive security programs.

These programs bring together a number of capabilities, including intelligence and information-sharing protocols; organizational and communitywide threat and vulnerability assessments; clear security policies and procedures; physical security measures; best-practice security training for clergy, lay leaders, professional staff, and all members of the community; and the development of close partnerships with law enforcement. They have been enhanced by various strategies and tools, from surveillance cameras to sophisticated communications systems. Perhaps one of the most visible elements of the strategies employed by organizations and facilities is the engagement of private security companies and contracted security staff.

At the end of the day, are these firms necessary? How much of a difference do these firms make? Is the Jewish community meaningfully safer, or is money wasted by engaging them?

On the one hand, the growing use of private security companies to protect America's faithful has, in many cases, strengthened coverage and improved flexibility with solutions that can scale up or down based on the impending threat. On the other hand, reliance on outside security can be fraught with risk.

Regulations governing private security officers are inconsistent across the United States and even within individual states. Training requirements and practices vary widely. Meanwhile, a lack of professional standards has meant that many of the security officers protecting our sacred spaces are ill vetted, ill equipped, and ill prepared. Some critics contend they can increase risk. Or even become armed mini-militias. As our primary recommendation makes clear: We must give more rigorous consideration to the selection, training, and oversight of the security officers hired to protect our communities of faith.

This white paper provides a roadmap for organizations seeking to strengthen an existing security program or establish a new one through the use of security officers. It offers a set of key questions and best practices that can help drive the conversation related specifically to security officers at every step along the way. Among the topics it covers:

- Identifying your organization's security needs.
- Formalizing your organization's security proposal.
- Hiring and vetting private security officers.
- Developing a security officer training program.
- Creating sustainable partnerships with local law enforcement.

Our white paper was developed by a panel of leading security professionals convened by the Secure Community Network (SCN), the official safety and security organization for the North American Jewish Community. Although it is written from a Jewish perspective, we believe that its insights are broadly applicable to all. Our hope is that it can serve as a valuable resource for many faith-based institutions, which are confronting similar security challenges.

The purpose of this paper is to help organizations that hire private security officers do it the right way. It can be tricky, but with the right questions asked and answered, the safety of the Jewish community can indeed be enhanced.

A ROADMAP FOR SECURING OUR SACRED SPACES

Traditionally, the face of security at many Jewish institutions and other communities of faith has varied widely: a volunteer receptionist, a member of the community or clergy, a facility worker or groundskeeper, or in some cases, a local police officer on detail for a special event. Today, as the responsibilities of our houses of worship, schools, and community centers have vastly expanded — and the need for more robust protection and an understanding of different types of issues and incidents, has grown alongside rising threats — many organizations are increasingly engaging outside private security for help.

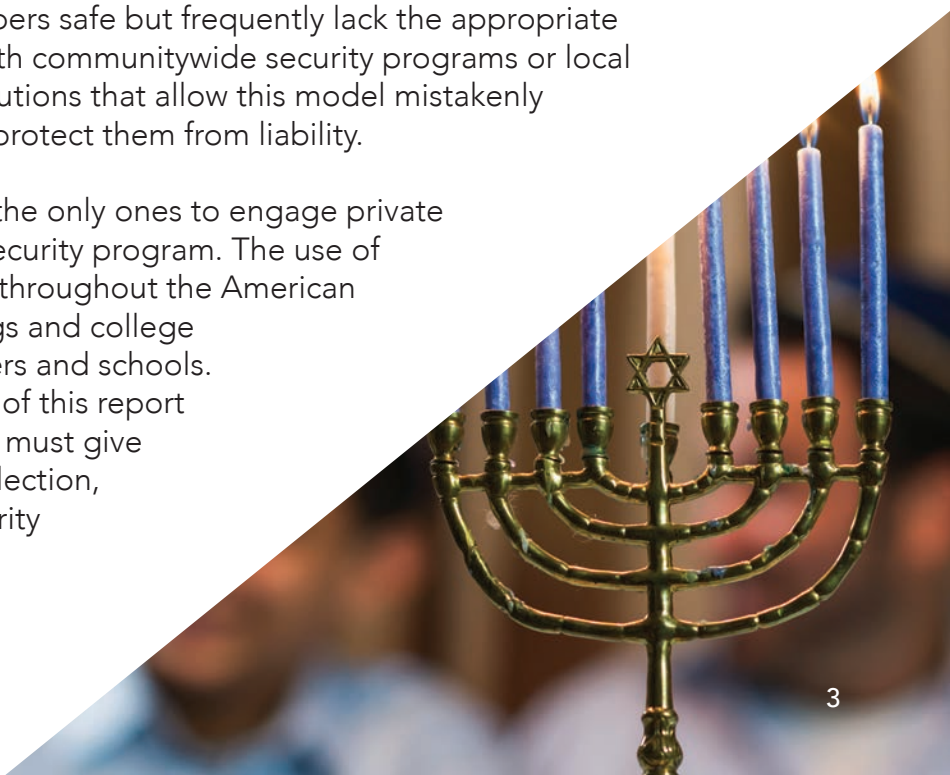
So far, the results have been mixed. On the one hand, the use of private security to protect America's faithful has, in many cases, strengthened coverage and improved flexibility, with solutions that can scale up or down according to scheduled events, threats, or incidents.

On the other hand, it can be fraught with risk. Government regulations, at all levels, governing private security officers are woefully inconsistent. Training requirements and practices vary significantly from state to state. Insurance liability, especially for armed protection, is substantial.

Meanwhile, inadequate professional standards have meant that many of the security officers protecting our sacred spaces are ill vetted, ill equipped, and ill prepared. In some cases, they themselves can present a threat.

Within the Jewish community alone, there are plenty of recent examples. In Pennsylvania, a private security officer at a large synagogue was terminated after smoking marijuana on the job. In Florida, a private security officer at a Jewish day school was caught sporting a wristband for Proud Boys, an organization whose members are frequently associated with white supremacist beliefs. The guard was promptly removed from his post. In another case, a private security officer was found publishing antisemitic statements on social media while ostensibly keeping watch at a community event. Meanwhile, a small but growing number of congregations are outsourcing security to armed volunteers — effectively creating mini-militias that aspire to keep their members safe but frequently lack the appropriate training or the proper coordination with communitywide security programs or local law enforcement. In many cases, institutions that allow this model mistakenly believe that such unofficial programs protect them from liability.

Of course, Jewish institutions are not the only ones to engage private security officers as part of an overall security program. The use of private security officers is widespread throughout the American economy — from commercial buildings and college campuses to secular community centers and schools. As a result, the core recommendation of this report has broad applicability: Organizations must give more rigorous consideration to the selection, training, and oversight of private security officers that are hired to keep their communities safe.



DRIVING THE SECURITY DISCUSSION: COMMON QUESTIONS, UNIQUE NEEDS

While the experts convened to develop this report believe that establishing comprehensive standards and/or a national training and certification program related to private security officers would be beneficial, this white paper stops short of establishing formal requirements or endorsing a single approach.[1] That is because there is almost never a one-size-fits-all security solution; every community is unique. Instead, this white paper aims to provide a set of guiding principles and key questions that can help drive the security conversation among organizations within the Jewish community and other communities of faith who aim to hire security officers. Among them:

- How can Jewish and other faith-based organizations most effectively use private security officers as part of a comprehensive security plan?
- What are best practices for engaging with outside private security companies?
- What are best practices and procedures related to hiring, training, and managing private security officers?
- What are the trade-offs between an armed and unarmed security team? What are the primary roles and limitations of each?
- How can private security officers most effectively partner with local law enforcement and community officials?
- How can innovative security models help maximize the resources a congregation or community has?

Congregations, clergy, and community leaders must place these questions at the center of their security and strategic planning discussions and ultimately answer them for themselves.

However, as the official safety and security organization for the North American Jewish Community, the Secure Community Network is committed to offering the best, most informed advice to those exploring security options. We believe the considerations outlined in the pages that follow can serve as a valuable resource. The insights are based on the input of top experts in the law enforcement and security fields, who convened at SCN's invitation to provide counsel to communities seeking the right security solution for their needs. Organizations can — and should — work with their local Jewish Community security director or regional security Advisor, along with law enforcement, to develop a strategy and plan that will work for them.

> **"Hiring private security officers is a tactic, not a strategy. It's a critical element of a comprehensive security plan, but it is not a security plan in and of itself."**
>
> **Michael Masters**, National Director and CEO, Secure Community Network

[1] Currently, the most comprehensive widely recognized national standards for private security officers are voluntary industry guidelines outlined by ASIS International, a professional organization by and for security professionals, that were initially released in 2004 and then updated in 2010 and 2019.

SCN WHITE PAPER CONTRIBUTORS

- Shawn Brokos, Director of Community Security, Jewish Federation of Greater Pittsburgh
- Brandon del Pozo, Former Chief, Burlington Police Department
- Steve Eberle, Regional Security Director, Secure Community Network
- Kurus Elavia, President, Gateway Group One
- Robert Graves, Regional Security Advisor, Jewish Federation of Greater Washington, Secure Community Network
- Jim Hartnett, Director of Community Wide Security Initiative, Jewish Federation of Cleveland
- Gil Kerlikowske, Former Commissioner, U.S. Customs and Border Protection
- Dan Levenson, Deputy Director, Communal Security, Combined Jewish Philanthropies — Boston
- Kathy O'Toole, Former Chief, Seattle Police Department
- Brad Orsini, Senior National Security Advisor, Secure Community Network
- Robert Wasserman, Senior Vice President, Jensen Hughes
- James Wasson, Security Director, Jewish Federation of Greater Phoenix
- Jeremy Yamin, Vice President, Director of Security and Operations, Combined Jewish Philanthropies, Boston

HISTORY AND MISSION OF SECURE COMMUNITY NETWORK

The Secure Community Network, a nonprofit 501(c)(3), is the official safety and security organization of the Jewish community in North America. Founded in 2004 under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations, SCN works on behalf of 146 federations, the 50 largest Jewish nonprofit organizations in North America, and over 300 independent communities, as well as with other partners in the public, private, nonprofit, and academic sectors to ensure the safety, security, and resiliency of the Jewish people.

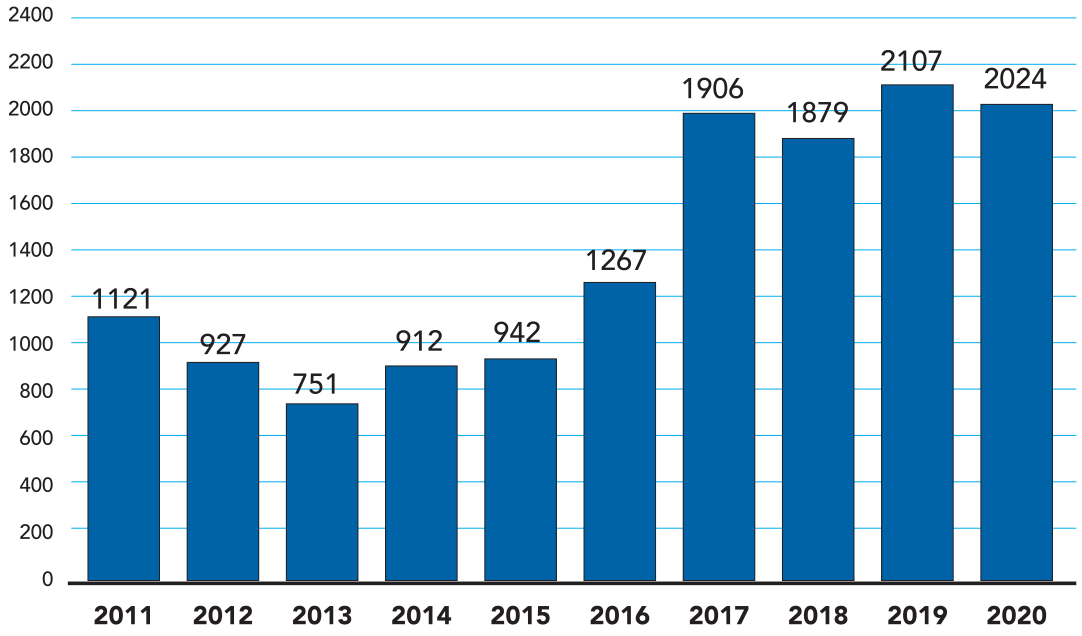
SCN serves as the Jewish community's formal liaison with federal law enforcement and coordinates closely with federal, state, and local law enforcement partners on safety and security issues related to the Jewish community; through the organization's Operations Center and Duty Desk, SCN analyzes intelligence and information, providing timely, credible threat and incident information to both law enforcement and community partners. SCN's team of law enforcement, homeland security, and military professionals proactively works with communities and partners across North America to develop and implement strategic frameworks that enhance the safety and security of the Jewish people. This includes developing best-practice policies, emergency plans, and procedures; undertaking threat and vulnerability assessments of facilities; providing critical, real-world training and exercises to prepare for threats and hazards; offering consultation on safety and security matters; and providing response as well as crisis-management support during critical incidents.
SCN is dedicated to ensuring that Jewish organizations and communities, as well as life and culture, can not only exist safely and securely, but flourish.

ADDRESSING A GROWING THREAT

From synagogues to schools, and from camps to community centers, the need for a stronger security presence at faith-based institutions is more urgent than ever. Amid a global wave of antisemitism, the frequency and lethality of mass shootings and other violent attacks have grown significantly over the last decade — not only for the Jewish community but many other communities of faith. Despite the temporary closure of many faith-based institutions during the global pandemic, the number of religiously motivated incidents targeting the Jewish community remains at alarming levels.

According to the Federal Bureau of Investigation's most recent hate crimes report, close to 60% of all religiously motivated hate crimes were directed at the Jewish community. While many religious institutions, schools, and university campuses shut down and large, in-person gatherings were strongly discouraged, real-world offenses motivated by Jewish bias remained high. Some of the most flagrant and inflammatory incidents of antisemitism during the pandemic shifted to be online, where hate speech flourished. Indeed, the FBI report found the number of hate crimes targeting Jews was nearly six times the number of incidents targeting the next most impacted group. Meanwhile, the Anti-Defamation League, noting a small decrease in antisemitic incidents in 2020 from the prior year, still found such cases were at their third-highest level on record since it began tracking antisemitic incidents in 1979.

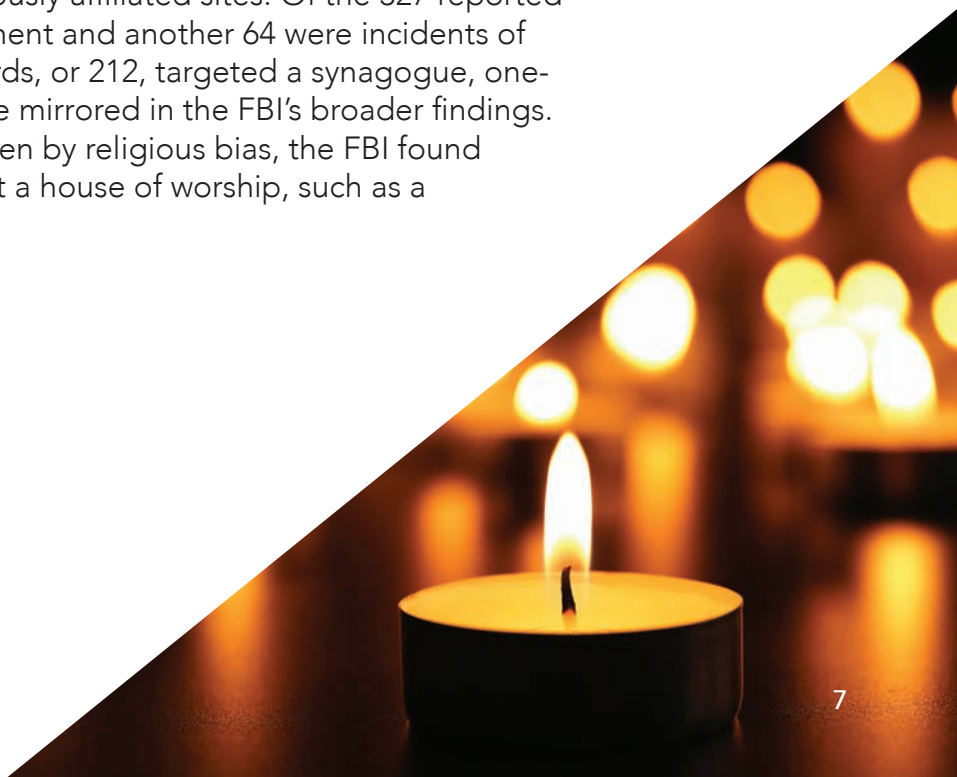
Antisemitic Incidents: U.S. – Over the Last Decade | 2011-2020



Source: ADL Report (2021).

NEW THREAT DYNAMICS, NEW SECURITY CHALLENGES

Of note, the threat of antisemitism appears to be expanding beyond the synagogue gates. For 2020, the ADL reported a 40% rise in antisemitic incidents at a broad array of Jewish institutions, including Jewish community centers, day schools, and other religiously affiliated sites. Of the 327 reported incidents, about 264 involved harassment and another 64 were incidents of vandalism. And while roughly two-thirds, or 212, targeted a synagogue, one-third did not. This trend appears to be mirrored in the FBI's broader findings. Of the 1,174 hate crime incidents driven by religious bias, the FBI found that fewer than one in five occurred at a house of worship, such as a church, synagogue, or mosque.



While antisemitism and other religiously motivated hate crimes tend to generate the most attention, another factor contributing to the need for protection at our faith-based organizations is so-called insider threats. This includes the personal troubles — whether related to a mental health issue of the individual or a domestic issue that manifests itself outside the home — that a member of the community, staff, or faculty may bring into a house of worship, school, camp, or social center, regardless of whether an institution is affiliated with the Jewish community. Meanwhile, as inherently inclusive organizations, many Jewish institutions offer social service initiatives that intentionally embrace such community members in need. The result is that faith-based institutions are often on the front lines of societal challenges, such as mental health issues, immigration, and refugee service provision as well as relocation programs, drug usage, and domestic abuse.

"Everyone is attuned to the potential of outside threats, but they don't think about the security challenges that arise internally from people who bring their life issues into the institution."

Shawn Brokos, Director of Community Security, Jewish Federation of Greater Pittsburgh

Faced with these new dynamics, today's Jewish communities are grappling with how to most effectively build a security program that gives their members confidence and calmness and, most of all, keeps them safe. Moreover, they must factor in an additional layer of complexity arising from the growing diversity of North American Jews. Almost one in 10 Jews identify with racial or ethnic categories other than "non-Hispanic White" and approximately one in five Jewish adults live in a multiethnic or multiracial household, according to a recent Pew study of the U.S. Jewish community.[2] That situation has resulted in the need for many organizational leaders to consider a much broader range of perspectives when it comes to law enforcement and security, given the diversity of lived experiences of their members, guests, and staff.

Of course, there are many other best-practice recommendations and hard-won lessons that can strengthen security for our diverse Jewish community and many other communities of faith. We share some of them in the pages that follow.

[2] Pew Research Center, "Jewish Americans in 2020," 2021, https://www.pewforum.org/2021/05/11/jewish-americans-in-2020.

IDENTIFYING YOUR ORGANIZATION'S SECURITY NEEDS

Those who assume a security role at faith-based institutions often have vital, expansive, and multidimensional roles. They often must be guards and gatekeepers, standing vigilant for suspicious behavior. They must be emergency responders, whether it is delivering first aid or ushering community members to safety in a crisis, such as a fire or an attack. In many communities, they are customer-support representatives. Private security officers often provide the first impression of an organization when they assist with directions or welcome visitors with a friendly "hello." They are also important liaisons with local law enforcement and public safety personnel, sharing their observations and intelligence with respect to the communities they serve.

As we observed in our initial white paper, "Firearms and the Faithful," private security officers may also be a critical solution for religiously affiliated organizations seeking an armed security

"This paper reflects the insights of leading security experts, law enforcement officials, and the professional security directors working on behalf of the Jewish community across North America. Their wisdom and pragmatic advice strengthen the safety and security of our community and its members."

Brad Orsini, Senior National Security Advisor, Secure Community Network

A POINT ON TERMINOLOGY: WHY 'PRIVATE SECURITY OFFICER'?

Since at least 2004, when ASIS International, a global organization by and for security professionals, first published its *Private Security Officer Selection and Training Guideline*, the term "private security officer" has been the industry standard term for what is commonly referred to as a "security guard." This standardization of terms is also reflected in the regulatory guidelines of many jurisdictions. While many law enforcement professionals will note that affixing the term "security" to an individual or service is appropriate only when the person is trained and equipped to provide the same, notably with a firearm, for consistency in this document and based on the above, the term "private security officer" is used throughout this publication.

presence in or outside their facilities.[3] Engaging a private security company may provide access to a scalable team of officers who are trained, licensed, and insured to carry weapons. However, some faith-based groups — for a mix of reasons — may have unarmed officers. What is clear is that there is never a one-size-fits-all solution. Before moving forward to engage a private security company, an organization should start by assessing its security needs, operating procedures, and community sentiment.

Within the Jewish community, many organizations have their own security committee that can help facilitate this conversation. Increasingly, Jewish federations will often have a community security director or regional security Advisor, often working with or through SCN, who can help direct or provide context for these discussions and serve as a useful sounding board.

So, what questions should organizational leaders ask? By defining the strategic objectives upfront and then determining the role that security officers can play in meeting them, organizations can more effectively marshal limited security resources. Here are a few questions that can help you get started:

[3] Secure Community Network, "Firearms and the Faithful: Approaches to Armed Security in Jewish Communities," 2019, https://securecommunitynetwork.org/resources/institutional-safety-and-security-library/houses-of-worship/firearms-and-the-faithful.

KEY CONSIDERATIONS FOR ASSESSING YOUR ORGANIZATION'S SECURITY NEEDS

What is the risk profile of your organization?

There is no single factor or piece of information that holds the key to understanding the level of potential risk or threat your organization may face. Instead, you must consider a range of elements to develop a more realistic, complete, and ultimately useful understanding of existing and potential threats. Among areas to consider:

What is the prominence of your organization?

Does your institution receive regular media attention within the Jewish community or the broader public? What is the nature and frequency of the programs and events offered? What is the level of social or political activism by clergy or lay leaders both on- and offline? Are there well-known congregants? For example, a synagogue that regularly hosts controversial speakers and shares the content online is more likely to draw attention — positive or negative — than one that has a minimal social media presence and does not host public events. Similarly, an Orthodox synagogue may attract more general attention because its members — who wear distinctive clothing — may be more outwardly visible. Given that a broad array of Jewish organizations have drawn the attention of violent extremists and other types of criminals, it is important to take into account all the aforementioned factors regardless of an institution's denomination, location, or size.

What is the physical infrastructure of your facility?

Have you conducted a "threat, vulnerability, and risk assessment" (TVRA) of your organization, to include the physical infrastructure? Are there any unique characteristics of the site? What is the nature of access points, and how might that affect staffing levels? How are you using technology, such as surveillance cameras or access control, as part of a comprehensive security solution?

What is the impact of current events on the overall threat environment?

How often is your organization and/or facility in the news? Does it take controversial advocacy positions or have prominent individuals associated with it? Are there local, national, or global events that might make it a potential target of terrorism or other hate-related crimes? Other concerns may be closer to home. For example, what is the general level of crime in the neighborhood where your institution is located?

> **"Global, national, and local events can certainly impact security threats from day-to-day. An organization should consider a tiered approach that starts with minimum standards, takes into consideration the unique characteristics of the facility they are protecting, and then look at the timing."**
>
> **Kathy O'Toole**, Former Chief, Seattle Police Department

What do you want private security to accomplish?

Your organization should develop a clear picture of what success will look like over time, including the key objectives and performance metrics by which to measure it. Your organization should also develop a clear portrait of what it wants its security presence to look like, and it needs to make sure those objectives are aligned since they all will drive the specifications of the job and clear expectations for the security officers. Among the questions your organization might consider:

Does your organization want armed security officers, and is it willing to invest in training and more experienced personnel?

If your organization wants armed officers, what are its needs, expectations, and concerns? (An armed private security officer is often not an adequate substitute for an active law enforcement officer.) Armed security officers are not law enforcement officials; those who are not retired or off-duty law enforcement officers may lack necessary credentials, training, and experience. At the same time, this must be balanced with financial demands. Generally, you get what you pay for: The more stringent your organization's criteria, and the higher quality security team it desires, the greater the expense.

What sensitivities might your community members have to the engagement of private security officers?

Security can be an emotionally charged and complicated topic. Some communities may desire uniformed and/or armed contractors outfitted with the latest equipment, while others may be turned off by the prospect of having a strong police or police-like presence in a community center or house of worship. When deciding whether to employ an outside private security officer, your organization will want to consider the impact of generational differences within the community. For example, with 15% of Jews under 30 identifying themselves as nonwhite or multiracial,[4] this increasingly influential demographic may have different relationships with law enforcement and different ideas on how to address security concerns than a leadership committee made up of older constituents. Being cognizant of the diversity of views — and identifying solutions that can bridge them — should be top of mind.

[4] Pew, "Jewish Americans in 2020," https://www.pewforum.org/2021/05/11/jewish-americans-in-2020.

> **"Diversity and demographics impact how security officers and law enforcement need to approach the communities they protect."**
>
> **Robert Graves**, Regional Security Advisor, Jewish Federation of Greater Washington

Can the private security company scale with your organization's needs?

In general, larger private security companies will have more resources available. But regardless of size, your organization will want to learn about their potential capabilities. Among the questions security leaders should ask:

- Can your security provider routinely engage the same personnel for each engagement or deployment?
- Can your security provider offer additional security professionals and/or trained and licensed armed officers if the situation warrants?
- Does your security provider have extra patrol vehicles, if necessary?
- Does your security provider offer an integrated solution of personnel, physical security solutions, and technology tools as a contingency plan?
- Are these solutions applied in a cost-effective, complementary model?

Has your organization developed the right infrastructure to support the use of private security officers?

Signing an agreement with a private security company is an important first step. But managing the relationship — with your organization, local law enforcement, and the broader community — will be critical to the effectiveness of the relationship. Prior to engaging a private security company, your organization should:

- Designate a security committee and/or identified security director or liaison to coordinate efforts and evaluate performance of the private security company.

- Develop robust relationships with local law enforcement officials.

- Undergo educational and informational outreach with key committee members to fully understand the complexity of security arrangements.

- Develop a relationship with SCN or local federation or regional security directors/ Advisors to assist/advise on the process. SCN and the network of security professionals have a deep understanding of security vendors, law enforcement, and other organizations. This can help ensure your organization is getting services that meet their needs and can help verify the private security company as a reputable and trusted agency.

Does your organization have the resources to support ongoing security?

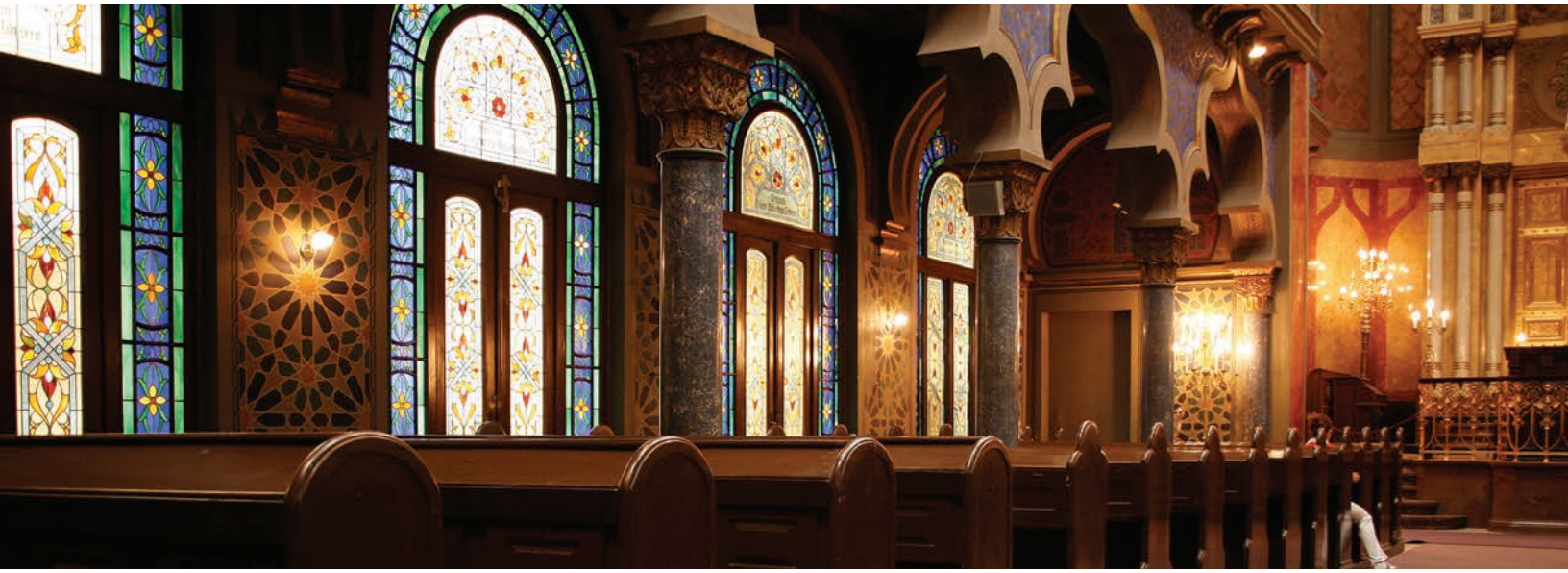
All too often, communities of faith mistakenly attempt to solve a short-term security problem with a long-term security measure, or they provide a short-term solution to a long-term security problem. (For example, in the wake of events such as a mass shooting, it may be better to escalate a security presence for a few weeks or months rather than commit to a long-term contract with a private security company.) Hiring private security officers is expensive, and the most forward-leaning organizations should honestly assess their ability to sustain the long-term cost of such a program. Here are a few other principles your organization should keep in mind before initiating a contract:

- If hiring private security officers is to be part of a comprehensive security plan, then it must be a core part of the organization's operating budget. It cannot be treated as a special, one-time expense.

- If your organization does not have the budget to make full-time security available, carefully determine which events or times of day warrant the presence of armed security and which do not.

- If engaging private security officers is a short-term measure, it is even more important to consider in advance your strategy for winding down their use. Adding security officers can be a welcome move; however, even if the precipitating crisis event has long passed, expect to address issues if and when your organization decides to take security officers away.

- If the funding for armed security comes from one individual or a small group, those people may feel empowered to set the terms of how security is provided and what the employed individuals are required to do, creating a potential source of conflict. Relying on SCN and the network of security professionals or hiring a security Advisor to oversee the program may help resolve this issue.



FORMALIZING YOUR ORGANIZATION'S SECURITY PROPOSAL

After identifying your security needs, the next step is to formalize the scope of work in a request for proposal, or RFP. Carefully defining the scope of work will give potential security providers a clear understanding of your organization's expectations, objectives, and the key performance metrics for which they will be held accountable. But perhaps equally important, it will also help clarify those elements for your organization too.

Generating a list of essential criteria in advance provides an initial layer of protection, ensuring that you get precisely what your organization needs and you don't get "upsold" on unnecessary capabilities. Moreover, by preparing in advance, your organization will send a strong signal to the private security companies competing for your business that your organization is confident, credible, and clearly understands the nature of its requests. That, in turn, should allow the security companies to be more responsive to concerns and anticipate potential issues or needs.

What is a request for proposal (RFP)?	A business document that announces a project, describes it, and solicits bids from qualified contractors to undertake the work.

As your organization seeks to define those criteria, here are some things to keep in mind beyond the standard billing rates:

> **"The best private security companies I've worked with appreciate high standards and hard questions because then they realize they're dealing with an experienced partner."**
>
> **Jeremy Yamin**, Vice President, Director of Security and Operations, Combined Jewish Philanthropies, Boston

KEY CONSIDERATIONS FOR DEFINING YOUR ORGANIZATION'S SECURITY CRITERIA

What are your organization's key performance indicators?

Any good RFP has key performance indicators, or KPIs, to measure performance, incentivize behavior, and hold the security company accountable. For example, a community might require the private security company to provide its workers with eight to 40 hours of paid training every six months. There also needs to be a consequence if the security provider does not meet the KPIs, either those it states it meets or that it is requested to meet. This might include a rebate of payments made on the contract, reimbursement of paid invoices, termination of the agreement, or a non-renewal of contract.

Given that performance will likely ebb and flow over time, as one security expert noted, the difference between a good security program and a bad security program is how you manage it. Therefore, it is critical that an organization's security leaders maintain open lines of communication with the security company's account manager(s) throughout the contract. Because these executives typically earn a significant amount of compensation based upon the renewal of your contract, they have strong incentives to ensure you are pleased with the service. They can also serve as effective internal advocates for making changes.

What types of accountability does your organization desire?

Today's security companies can provide their officers with smartphones or other devices that contain post orders, facility floor plans for evacuations, emergency communication protocols, and contact information for key personnel. Meanwhile, RFID and GPS technology can help verify that security officers have completed all the tasks on their list. Your organization should clearly specify in its RFP what technologies are desired.

If your organization does not know what technologies it needs, consider consulting your community's security Advisor and SCN for resources to help. Legal counsel may also be helpful in providing guidance from a legal liability perspective.

What are your organization's uniform preferences?

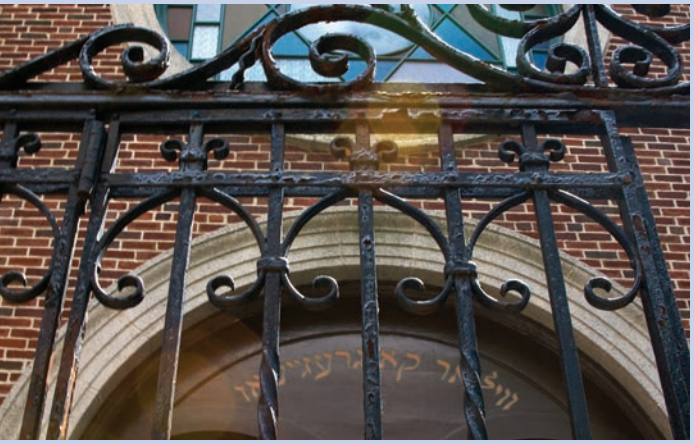
The private security company should provide information on any uniform options. Your organization should then confirm what you do or do not want your security team to wear and, if so, how the officers appear.

What constitutes overtime compensation?

State laws affect overtime payment, such as when private security personnel work on a federal or state holiday. Legal counsel should be able to provide the overtime requirements that should be detailed in the RFP.

Are there any hidden red flags that your organization might learn of from peers?

As you evaluate the RFP bids, it is crucial that your organization ask for references. Do not be afraid to ask for a list of names and contact information for other faith-based groups that use the security company your organization is considering.



BOSTON'S BEST PRACTICES FOR HELPING A DIVERSE GROUP OF ORGANIZATIONS ADDRESS THEIR UNIQUE SECURITY NEEDS

The Jewish community of the greater Boston area includes over 100 synagogues, 30 Chabads, 40 pre-schools, and 14 day schools, as well as more than a dozen Hillels and summer camps extending from the city to the Berkshires, and all the way up the Maine coast. Most had inadequate security resources and staff. So, when the Combined Jewish Philanthropies (CJP) of Greater Boston created its Communal Security Initiative, one of the first priorities of the new security director was to create a consistent yet customizable approach to address the region's diverse security needs.

What was the key to CJP's approach? Building a recommended security provider list and writing a model RFP that outlines critical requirements and responsibilities for all contracted security staff. Ultimately, CJP developed a list of reputable security firms that had experience working with Jewish institutions in the region as well as standard RFP language that could be easily adapted to meet any organization's unique needs. "We don't want to micromanage hundreds of institutions," said Jeremy Yamin, CJP's director of security and operations. "We want to provide simple guidelines and a framework for them to complete to set them up for success."

So, what are some best practices that the Boston CJP security leaders suggest?

Start by having your institution identify its most critical security needs.

Before drafting the RFP, make sure your organization's key security decision-makers[5] agree on elements of the proposal, including: Why is it necessary to allocate security resources? How frequently does your organization need professional security officers and/or police details — and for how long? What is its budget? Will your organization be using armed or unarmed security officers, or police details? Your organization should also identify an individual who is typically on-site and can coordinate security officer and/or police detail coverage as well as serve as a consistent point of contact for the security company and police department. Asking these questions in advance will go a long way toward setting up and maintaining a sustainable security program, which may or may not include security officers and/or police details.

Conduct an internal review of the completed RFP before its release.

If your organization has security, it has liability. So, make sure the appropriate organizational leaders vet and approve the RFP before it is broadly distributed externally. These individuals may include your organization's security subcommittee, legal counsel, or HR leader. Some organizations may have, or should consider, requirements or governance protocols around who reviews and may need to approve such documents.

Conduct an external review with friendly stakeholders before the RFP's release.

Consider requesting that the local police department or other trusted source review your RFP to ensure it comports with local law enforcement practices. Your organization may also want to share the draft with one or two subject matter experts who may be able to flag oversights or omissions before the RFP is broadly distributed.

Focus on hourly wages of the security officers — not just the billable rate your organization pays.

In the RFP, consider stipulating a minimum acceptable hourly wage paid to the security officer — don't just focus on the rate charged to the institution. A higher hourly wage will help make an assignment at your institution more attractive to the officers, help reduce turnover, and force the security companies to compete on lower administrative costs rather than competing by offering the lowest wage.

Provide clear post orders upon awarding the contract.

Upon engaging a security provider, those individuals from your organization who are responsible for overseeing and maintaining the relationship with the security company and its security officer(s) should conduct a walk-through of your facility with that firm's leadership. Those individuals should provide the security company with a list (ideally no longer than two pages) that clearly outlines your organization's expectations of the security officer(s) who will be on-site, including the scope of their responsibilities. These post orders should also describe the expected safety and communications protocols in the event of a medical emergency, nonviolent disruption, a deliberate disruption of services, and any other scenarios or events likely to occur while an officer is present.

[5] These decision-makers could include executive leadership, clergy, board chair, a board-level house or security committee, head of facilities, or some combination thereof.

NEW AND INNOVATIVE SECURITY SERVICES MODELS

The use of RFPs to solicit competitive bids from multiple service providers is a tried-and-true method for identifying the right private security company. This can allow a diverse group of member organizations to obtain the security services that best suit their needs. (See some of the lessons learned in the case study on Page 18.) Within the Jewish community, a growing number of organizations are experimenting with new and innovative security models that make use of the RFP.

For instance, in Washington, D.C., a loose confederation of Jewish organizations in the District, Maryland, and Northern Virginia are moving toward a so-called Co-op Model, in which they are governed by a common contract, but each group is individually responsible for paying for the services they use. Instead of independently soliciting competitive bids, participating organizations are directed to a list of prequalified private security companies that have met a set of criteria. And instead of each organization negotiating a unique contract, participants agree to abide by a master service agreement, also called a framework agreement. Under this arrangement, commonly used for the purchase of open-ended services, the parties agree to most of the key terms — such as

> **"The master service agreement serves as that first layer of protection so that a local community or organization does not entertain just anybody."**
>
> **Steve Eberle**, Regional Security Director, Secure Community Network

officer training criteria, insurance requirements, and officer billing rates — that will govern future transactions. (See some of the lessons learned in the case study on Page 22.)

This approach has several advantages. First, it allows all participating organizations to benefit from the expertise of security leaders who are experienced at negotiating these types of contracts. Doing so makes it less likely that the organizations will overpay or get upsold on services they don't need. Second, it enables all key terms to be negotiated upfront — not in a moment of crisis when an organization does not have much leverage. Third, it allows participants to reap significant benefits of scale from joining forces with their peers. Lastly, it helps prevent the "friend of the community" problem, in which a community may choose a vendor based on a pre-existing relationship, not its capabilities and performance.

At the other end of the spectrum, the Jewish Federation of Cleveland (JFC) established its own security entity and provides armed officers to many organizations within the community at subsidized rates. Even though it costs several million dollars a year to operate, JFC security leaders say that they would pay roughly the same amount or more if they engaged a private security company to supply officers — and are able to offer better protection, better resources, and a better trained team. (See some of the lessons learned in the case study on Page 32.)

Key to the success of the noted approaches is the coordination and expertise provided by a professional security Advisor. Whether provided by the SCN or a local federation, these individuals can provide critical guidance to ensure your organization's security program matches its needs.

IN FOCUS:

Lessons Learned From the Washington, D.C., Co-op Model of Security

Roughly a half-dozen, prominent Jewish organizations — including a synagogue, a day school, a nursing home, and a Jewish community center — are clustered around a small campus in a Washington, D.C., suburb in Maryland. Historically, these organizations independently engaged their own security staff. But for the last two years, they have been taking advantage of the game-changing benefits of quite literally joining forces: The security officers patrolling most of the campus's facilities are governed by a single contract, overseen by the same supervisor, and have their costs spread among the various organizations located there in proportion to their use.

And that was just the start. Today, nearly a dozen Jewish institutions across the D.C., Maryland, and Northern Virginia region are participating in what's known as a "security co-op model" — an arrangement that has been common among large property-management companies with multiple buildings in an area but unique among communities of faith. Moreover, the security Advisor for the Jewish community in the nation's capital is currently drafting a master service agreement with the campus security provider to standardize guard compensation and other key terms — giving virtually every Jewish institution in the Washington metropolitan area access to a similar deal.

Local security leaders see significant advantages to the shared services approach. For one, they can significantly reduce security guard costs for participating organizations — in some cases, helping lower the billing rate for unarmed security staff by more than 25%. That's in large part because of the purchasing power that comes through pooling the billable hours across several organizations and then forcing security providers to compete for a single contract, rather than bid on a bunch of small jobs. It provides flexibility too. Guard hours can be split among the program's various participants; for example, a synagogue that needed security for only a few hours during Shabbat services was able to split the guard's cost with a Jewish nonprofit, which employed that same guard during the work week. Likewise, a local Jewish day camp was able to engage a full-time security guard for its eight-week summer session since the security provider could easily redeploy that guard to work at another organization once camp ended. Third, it has led to lower turnover, greater consistency, and increased trust. Guards gain a deeper understanding of the culture, rhythms, and people who make up the Jewish community. Meanwhile, because they may work at one or two different Jewish sites, the guards become familiar faces among community members too.

What the model does not necessarily do is lead to the hiring of better guards. It's still very much a mixed bag, Washington security leaders note, when dealing with any outside security provider. However, establishing a master servicing contract can put in place some minimum training requirements and hiring qualifications. The fact is that larger security vendors, which typically pay a few dollars more per hour, are more likely to bid on larger contracts that may indirectly lead to more loyal and experienced officers as well as higher morale.

Washington security leaders also emphasize that it imperative to ensure there is a fair and competitive bidding process when awarding any large contract. And it's crucial that no community or organization rely on a single firm. Different security providers have different strengths. So, while many of the Jewish organizations in the capital region have a master servicing agreement with one provider for unarmed security guards, there are different providers for armed officers, which command a higher level of pay commensurate with their training.

Here are a few other key takeaways from Washington, D.C.'s security co-op model:

- Security services should be bought — not sold. Savvy organizations start by conducting their own assessment of their security needs — and then tell the provider what they want through the proposal process. Although it can be worthwhile to learn about a provider's full suite of capabilities, don't fall into the trap of being upsold on services that your organization doesn't need. An SCN Advisor or other independent security Advisor can serve as a useful resource in helping identify your security needs.

- Establish a single point of contact with your security provider. Request that the security provider assign an account manager responsible for all Jewish organizations using its services. This can facilitate improved communication and sharing of best practices among the security staff at all participating organizations while providing the Jewish community with a designated leader who can quickly address any issues that arise.

- Strike a balance between standardized and customized security solutions. While there can be significant benefits achieved by economies of scale, it's also important to recognize that each organization has unique needs. So, for example, instead of setting a single bill rate in a master service agreement, establishing a billing range allows for some flexibility and negotiation between the participants and the provider.

- Establish a clear and consistent process for billing. In general, it is easiest for the security provider to invoice a single client, such as a Jewish federation. However, it's generally cleaner if each organization receives a bill based on a determined percentage or formula that calculates its share. There's no one right way of doing this. Whatever you choose, however, it should be fair, transparent, and clear.

- Don't be shy about providing feedback to your security provider. Deliver clear, candid, and regular feedback to your security provider — including the things going right as well as wrong. A well-run security firm wants to know the good things so that it can appropriately recognize and reward outstanding employees. And, of course, it can't solve issues it does not know about.

UNDERSTANDING HOW YOUR SECURITY PROGRAM AFFECTS YOUR RISK

When putting together the RFP, your organization must not only pay attention to the upfront costs, but also be keenly aware of the hidden costs of potential liabilities. Oftentimes organizations will see engaging a private security company as a way of transferring risk and liability onto a third party. To be sure, a private security company must have insurance to cover potential liability. But that does not negate the need for your organization to have its own liability insurance too. To get a better handle on the potential liability consequences from a financial perspective, your organization should have a parallel conversation with its insurance and risk management Advisors. Among the questions your organization should ask:

KEY CONSIDERATIONS FOR ASSESSING YOUR LIABILITY

Are the following included in the private security company's insurance coverage?

- Workers' compensation, as required by applicable statute and employer's liability insurance
- Commercial general liability insurance
- Professional liability
- Automobile liability
- Excess-umbrella insurance, including terrorism coverage (which does not cover hate crime incidents)

In addition, your organization must also be listed as an additional Insured on the general liability, auto, professional, and umbrella policies. Your organization should reserve the right to request additional or revised contractor insurance information based on review and recommendation by the client's insurance provider. Always request a certificate of insurance from the contractor.

What is the risk exposure arising from your organization's facilities?

- If a person is injured while representing the facility and acting in an official capacity, is workers' compensation an issue?

- Does the facility carry the necessary amount of liability insurance to cover this specific security function?

How will the use of armed security officers affect your organization's liability?

- Does your organization's current insurance coverage even allow armed security officers?
- What if the on- or off-duty law enforcement officers are insured by their agency?
- Also, if the police department is protected by sovereign immunity, does liability fall solely on the organization?

UNDERSTANDING POTENTIAL LEGAL RISKS

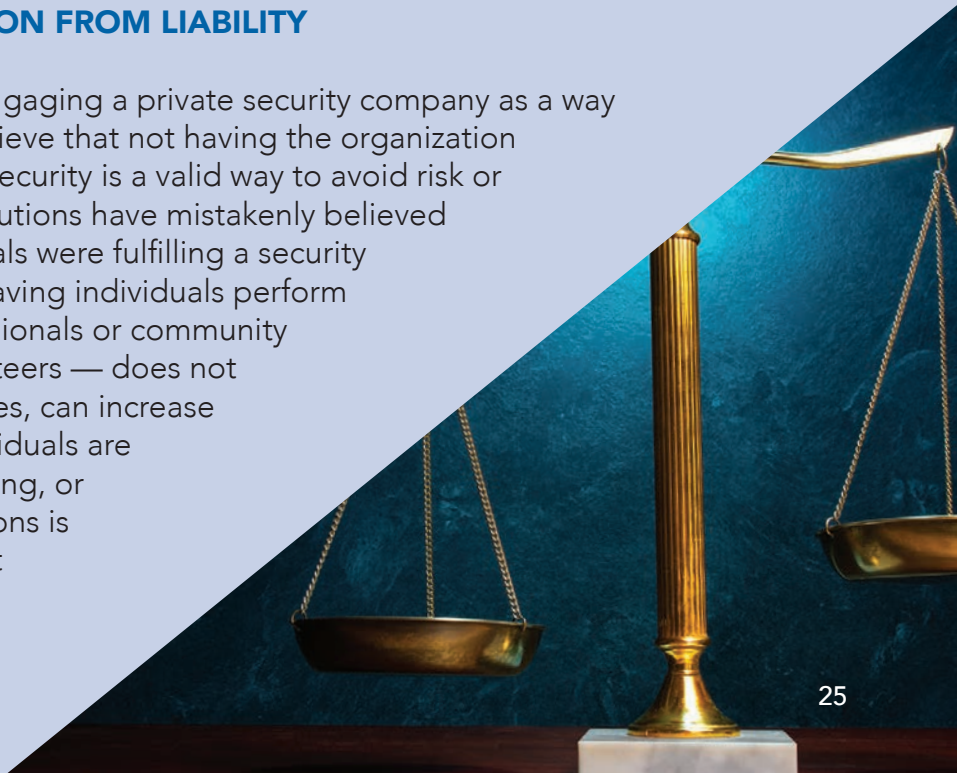
The participation of legal counsel is important to helping your organization assess potential legal risks. These can vary significantly based on the size, type, and location of your organization. Therefore, your organization's legal counsel should be tasked with identifying security laws applicable to the organization and be well versed in the regulations as they apply to its jurisdiction and activities. For example, a JCC day care facility in Georgia would have very different applicable laws than a federation office in California. On a national level, there are no safe harbors for nonprofit organizations, nor is there any set of safety and security rules or controls whose adoption can guarantee protection from liability. While the laws of each state may vary in this regard, the typical legal analysis looks at whether the organization has assessed and is managing security risks to a degree as would seem to be reasonable and appropriate, or as applicable to reasonably foreseeable risks.

In addition, your organization's legal counsel should ensure that its security objectives are consistent with its legal obligations. Counsel should also work with organizational leaders to focus on appropriate objections based on risk assessments and help establish a compliance assessment process. Other roles for legal counsel include the development and review of policies and contractual documents used as security safeguards and controls, working with security professionals to identify safeguards that may be required to meet the applicable standard of care, and ensuring the adequacy of security compliance documentation for evidentiary purposes. Your organization's leaders may also find the advice of legal counsel beneficial as it relates to their personal liabilities relating to security matters.

These multiple roles mean it is important to engage with counsel that have the appropriate level of expertise or can make use of outside counsel when dealing with potentially important security issues.

VOLUNTEERS ACTING IN A SECURITY FUNCTION DO NOT SHIELD AN ORGANIZATION FROM LIABILITY

While some organizations may see engaging a private security company as a way to transfer risk and liability, others believe that not having the organization or institution pay for or formally hire security is a valid way to avoid risk or liability. Other cases exist where institutions have mistakenly believed that not acknowledging that individuals were fulfilling a security function alleviated risk. To be clear, having individuals perform a security function — whether professionals or community members, and whether paid or volunteers — does not avoid risk or liability and, in many cases, can increase it. This can be particularly true if individuals are armed. The idea of not "seeing, hearing, or speaking" about individuals or functions is not an effective strategy. It can be not only costly, but also dangerous.



IMPLEMENTING YOUR ORGANIZATION'S SECURITY SOLUTION

Not only do security officers provide protection, but they are also often the first people a visitor interacts with at a house of worship, school, or community center. That's why it is essential that both the private security provider and the contracted security officers it employs be aligned with your organization's expectations, standards, and values.

Inconsistent requirements can make this challenging. Many states require mandatory federal criminal background checks for security professionals, but at least nine states currently do not. Likewise, many states require mandatory firearms training for armed security professionals, but 15 states do not. Similarly, the requirements for physical, vision, and psychological exams for armed security professionals vary from state to state.

AN INCONSISTENT APPROACH TO SECURITY HIRING AND TRAINING

There is no federally standardized training protocol for security officers in either the United States or Canada.

In 15 states, armed security officers can carry guns without firearms training.

In nine states, federal criminal background checks are not mandatory.

Fourteen states do not license or issue permits to armed security officer applicants.

Twenty-seven states do not check whether applications to be armed security officers are prohibited by court from possessing guns.

Only a handful of states require physical exams, vision exams, and psychological exams for armed security officers.

Oregon is the only state that checks to see whether an applicant with law enforcement experience has been fired for egregious behavior on the job, making that person unsuitable for armed security officer employment.

SELECTING THE RIGHT SECURITY PROVIDERS

In 2019, ASIS International published an updated series of guidelines for selecting and hiring private security officers in an effort to establish some national criteria, building on an initial report from 2004.[6]

Notwithstanding that report, there are still no minimum requirements. While this paper stops short of providing formal standards, we do believe it is useful to revisit our list of best practices as your organization considers, selects, and onboards its security team. In the next section, we offer some ideas for hiring and vetting private security companies as well as the security officers serving on the front lines.

[6] ASIS International, *Private Security Officer Selection and Training Guideline*, 2019. Available for purchase online on the ASIS International website (https://www.asisonline.org/publications--resources/standards--guidelines).

KEY CONSIDERATIONS FOR HIRING AND VETTING PRIVATE SECURITY COMPANIES

Are they a local or national security provider?

Although a local provider can bring familiarity with and insight into a community, your organization should consider whether it has the appropriate resources (additional capacity, armored vehicles, specialist services, technology solutions) to scale with the institution's evolving needs. Similarly, does a national provider understand local dynamics and community issues sufficiently to serve your organization? Similarly, does a national firm have adequate leadership presence in the jurisdiction to effectively support you, from a strategic perspective?

Does the security provider have ties to your community?

Hiring a security provider that has close ties to your community (or the leaders of your organization's security committee or board) may feel instinctively right. However, security experts caution against relying on these characteristics as the primary reason for engaging a particular security company. Instead, your organization should establish a set of minimum criteria first. Evaluating the proposal based on that selection criteria, rather than personal referrals, will provide your organization with the best chance of success. Personal relationships and community affiliations can also impede the ability to hold a contractor or service provider accountable. A larger or national security provider can generally hire these smaller security companies as subcontractors, and they would fall under their insurance umbrella. We believe this is a more prudent approach for organizations that have prioritized hiring smaller, minority-, woman-, or veteran-owned companies; it also provides more flexibility to access additional security resources if a situation warrants it.

What is the security provider's reputation?

- Can the security company provide at least five years of financial statements?
- Can the security company provide a good standing letter?
- Can the security company provide a license from the state?
- Has the security company encountered any lawsuits over the last five years?
- What is the security company's Dunn & Bradstreet number?
- Can the security company provide references from peer organizations and local law enforcement?

How does the security provider manage its private security officers?

- What is the security provider's bill rate, that is, the amount it will charge your organization?
- What is the security provider's pay rate, that is, the amount it will pay its private security officers?
- How often does the security provider run criminal records checks on employees? Do they check social media accounts of their employees ever or regularly?
- Does the security provider have any hourly requirements for its private security officers?
- What are the security provider's standard policies and training program? Is there a minimum or set number of training hours its private security officers are required to attend annually?
- What benefits does the security provider offer its private security officers?
- How much turnover does the security provider (locally, regionally, and nationally) have each year?
- Can the security provider explain how it handles internal complaints?

KEY CONSIDERATIONS FOR HIRING AND VETTING INDIVIDUAL PRIVATE SECURITY OFFICERS

In general, compliance with state and federal law should be the starting point of any selection criteria. The 2019 ASIS Private Security Officer Selection and Training Guideline provides a generic framework and illustrative examples of criteria organizations might consider. Although these guidelines can provide a solid foundation for any minimum standards, we encourage organizations to consider additional criteria as part of a holistic assessment. Below are some considerations highlighted in the 2019 report.

2019 ASIS INTERNATIONAL EXAMPLE SCREENING CRITERIA [7]

General Criteria: Candidates meet minimum legal requirements for armed and unarmed security, as specified by jurisdictional law, with provisions that the candidate must be able to perform the duties required of the position.

Authorization to Work: Candidates are compliant with jurisdictional legal requirements to work.

Personal Information: Candidates submit their current and previous residential addresses and phone numbers for at least the last seven years. (See parenthetical remarks under Social Security Number.)

Social Security Number: Candidate's name and Social Security Number are verified. (Additionally, consideration may be given to conducting a Social Security Number trace to determine if the number has been actively issued and is not retired, as well as to obtain an address history. The address history should be compared against addresses given on the application and used to verify that criminal record checks have been conducted for all required residence addresses.)

Education: Candidates possess a high school diploma, GED, or equivalent. Also, the applicant should demonstrate an ability to read, write, and speak English and the language(s) most appropriate to the assigned duties. Additionally, consideration may be given to the administration of a validated aptitude test for security officer applicants.

Criminal History: Candidates must not have been convicted of or pled guilty or no contest to a felony or job-related crime for at least seven years immediately preceding the candidate's date of hire. Any felony conviction discovered in the course of conducting the search should also be considered relevant to the candidate's qualifications for the position. Armed security officer candidates must not have been convicted of a state or federal misdemeanor involving the use or attempted use of physical force or the threatened use of a deadly weapon.

Employment Verification: A candidate's current and previous employers' addresses and phone numbers for at least the last seven years are verified. Candidates with prior military service may be required to provide form DD-214.

[7] Copyright 2019 ASIS International. Source: ASIS International, *Private Security Officer Selection and Training Guideline*, 2019. Used with permission.

Registrations/Licenses and Certifications: Candidate-provided license, registration, credential, or certification information is verified with the appropriate agency. (Compare given information on licensee's name and address, licensing board, or agency name, license type, license number, status, and original issue date. Note any negative license actions or sanction if provided by the agency.)

Fingerprints: Candidates submit a fingerprint card or electronic fingerprints to be processed for a criminal history check. Whenever possible, consideration should be given to the use of a national fingerprint identification database.

Drug Screening:

- Pre-employment: Candidates undergo a drug screen.
- Postemployment: Random drug testing, where permitted by state law and employer policy, should be conducted using a valid random testing methodology.

Drug screenings should be consistent with jurisdictional laws and may include on-site drug screens administered on company premises, job sites, and/or clinics.

Photographs: Candidates submit a recent (within the past 30 days) passport-size photograph for purposes of identification and registration/licensing.

Credit Check: Candidates undergo a credit check, where allowed and appropriate.

Physical and Mental Fitness: Candidates have the ability to perform essential job functions with, or without, reasonable accommodations.

Motor Vehicle Registration: For any private security officer with driving responsibility in a motorized vehicle (not limited to those driving company vehicles), consideration should be given to conducting an annual motor vehicle registration check (also known as MVR or DMV check) to verify license information (type or class of driver's license, full name, and address at the time of last license renewal), restrictions or violations, convictions and license revocations, automobile insurance cancellations, and accidents.

OTHER PRIVATE SECURITY SELECTION CONSIDERATIONS

Is your private security officer fit to serve?

Security experts have found that psychological testing, though costly, can be a useful and appropriate tool. This is especially the case when it comes to determining the mental fitness of potential armed security officer candidates who will be authorized to carry a live weapon. In addition, your organization may want to consider imposing certain job-relevant physical fitness requirements, such as the ability to stand and/or sit for extended periods, run a specified distance, climb stairs, or lift a specified weight.

Does your private security officer have a concerning past?

One issue that frequently arises in the vetting process is that most private security companies screen only for criminal convictions. That means that a prospective security officer, who may have been arrested for a serious crime, will evade scrutiny if he or she was never convicted. To address this gap, your organization should consider including a workmanship integrity requirement.

What is a Workmanship Integrity Requirement?

Criteria set by both the organization and the security guard company prior to start of contract to ensure the quality of services remains adhered to. These criteria should be measurable and have a process for evaluation that should be completed yearly.

Does your private security officer comply with your organization's social media expectations?

Social media postings can reveal important aspects of a security officer's beliefs and values, which might be embarrassing and potentially dangerous to your organization. For example, one Jewish organization discovered that a security officer it hired was publishing antisemitic posts while on the job — and was promptly removed from the post. Many organizations have developed standards for appropriate social media posts and aggressively monitor that activity. However, at a minimum, the social media accounts and posts of potential candidates should be subject to an initial and ongoing review to ensure they are not contrary to the values and policies of your organization.

How much hiring discretion does your organization have?

Organizations should have the right to meet any security professional they engage before they approve that person's employment, although many do not exercise it. Clergy, congregation, and community leaders should seize this opportunity to ensure they are getting the personnel they want.

STRENGTHENING SECURITY TRAINING

In contrast to most law enforcement roles, there is no formal standardized training for security officers. No federal guidelines exist, and training requirements vary considerably from state to state. Twenty-two states have no training requirements for unarmed security professionals — and 15 of those have none for armed security professionals either.[8]

Security officers protecting houses of worship and other faith-based organizations may require additional training on top of what is typically provided by the private security companies that hire them. For example, for security officers protecting a synagogue, information sessions on religious customs, practices, and traditions can be highly valuable. Additionally, sessions on community engagement and cultural sensitivity may be desirable beyond the tactical and emergency training these professionals frequently receive.

Although this paper does not attempt to prescribe a set number of training hours, we believe that communities are far better served when their security personnel have the chance to develop and refine their skills. In general, the length and content of pre- and postassignment training should be tailored to the unique demands of the job.

Of course, your organization must balance this outlook with the reality that training may seem expensive — and the more training hours a security professional accumulates, the more compensation they are likely to command over time. On top of cost concerns, your organization must balance the desire for training with the reality of needing to keep its security personnel at their posts. One way to bridge this gap is to require the training as part of the RFP process, shifting the requirement to the company. Working through a collective service model as a community, instead of just one organization, can provide leverage for the community to demand and receive better service, at reasonable value. Moreover, through the RFP process, your organization can require the company to send its personnel to the community security director or other resource to receive the noted training.

So, what type of training is most relevant to security professionals working with communities of faith? Given the wide-ranging nature of the role, it's not surprising that there is a plethora of topics and approaches.[9] While no private security company should be expected to offer every course, it should provide a broad mix of training options so that clients can pick and choose the sessions that best meet their security needs.

EXAMPLES OF POTENTIAL SECURITY OFFICER TRAINING PROGRAMS

Security Awareness: How the security officer's role fits into a comprehensive security plan
Active Assailant: Crisis-management training for violent attacks
Situational Awareness: Behavioral awareness training and screening tactics
De-escalation Training: Provides tools and options to manage various situations
Implicit Bias Training: Management of unconscious biases and stereotypes
Incident Response/Crisis Management: Preparedness training and protocols
Use of Force: Training for armed members of the security team

[8] Jenni Bergal, "In Many States, Security Guards Get Scant Training, Oversight," *Stateline* (Pew Charitable Trusts blog), November 10, 2015, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/11/10/in-many-states-security-guards-get-scant-training-oversight.
[9] Beyond classroom and online seminars, security experts recommend the use of tabletop exercises and crisis event simulation for training. The latter two are considered best-in-class methods for adult learning.

IN FOCUS:

HOW CLEVELAND'S FEDERATION CREATED A COMPREHENSIVE IN-HOUSE SECURITY PROGRAM

Most Jewish communities are in the process of addressing their community security needs. The Jewish Federation of Cleveland (JFC), on the other hand, has been investing significant resources into industry-leading security measures for close to a decade — and now has its own proprietary security force. In what may offer a preview of a comprehensive security model for other Jewish communities, the Federation established JFC Security LLC, a separate security company, licensed by Ohio's Department of Public Safety, for its officers to carry firearms. JFC undertook a series of sweeping measures — from hiring several former police chiefs to acquiring a fleet of mobile patrol vehicles — to strengthen protection. The result: Today, the Cleveland area has perhaps the most sophisticated security officer program of any Jewish community in the United States.

To be sure, Cleveland's security program — in the aggregate — can appear expensive: It requires an operating budget of several million dollars per year and initially was almost entirely funded by the Federation. But JFC Security leaders say that their costs are currently not much higher than if they paid an outside security firm for its services. Moreover, they assess that if each institution pursued a comparable level of security, individually, overall costs would actually be much higher. The current program therefore allows for efficiency in spending while, JFC leaders noted, resulting in a more committed, resourced, and experienced guard force over the long haul. Ultimately, the JFC plans to phase out the bulk of the security subsidies for direct guard service to most Jewish institution clients so that the program can largely sustain itself, while maintaining funding for centralized community security activities.

Cleveland's security program has been years in the making. Following the 9/11 attacks, Cleveland's Federation began hiring former police officers to provide armed security in the lobby of its building. A decade later, in the wake of several high-profile school shootings, Federation officials believed they needed a more visible security presence and standardized approach, and they began coordinating with community police departments in the area to ensure that each Jewish day school was staffed with an off-duty police officer during hours of operation.

Working with outside legal and insurance Advisors, in 2015, the Federation established its own security guard company, segregating the liability of the unit by making it a limited liability corporation (LLC). By 2017, JFC Security LLC was run by Jim Hartnett, a former FBI agent, and a deputy director who was a former chief of police for a local municipality with a sizable Jewish community. Together, they further professionalized the Cleveland Jewish community's approach to security: providing standard uniforms and equipment to guards; establishing policies governing the use of mobile patrol vehicles and officers' conduct; and developing a comprehensive training program (including active shooter, bomb threat, stop-the-bleed, detecting suspicious activity, and proactive patrolling) for all JFC Security officers. Additionally, they instituted a community training program to increase the culture of security among community stakeholders.

Today, the JFC Security ranks have significantly increased and now include former police officers, FBI agents, SWAT team members, and even a handful of police chiefs. The number of uniformed officers now rivals that of area suburban police departments — a ramp-up achieved largely through word-of-mouth recruiting and close ties to the region's law enforcement networks.

Moreover, over time, the Jewish community's security infrastructure has been strengthened too. For example, working closely with several local car dealers, JFC Security acquired donations of mobile patrol vehicles. It also aggressively applied for state and federal security grants, securing several million dollars in funding to improve target hardening of the community's synagogues, schools, and agencies. These capital grant dollars have allowed for the provision of emergency radios, the installation and upgrading of technology infrastructure, and the establishment of centralized camera monitoring at a regional dispatch center. JFC Security now has a full-time IT staff member to oversee security technology projects, bids, and proposals.

Of course, Cleveland's security model may be difficult to replicate. Not every Jewish community has the philanthropic funding base to sustain such a comprehensive program. In addition, Cleveland's Jewish community is, for the most part, geographically self-contained. Many of its Jewish institutions are clustered within a few distinct neighborhoods. That means it can more quickly reap the benefits of scale.

But other aspects of Cleveland's approach can be duplicated — especially the strong relationships and the trust that JFC Security has developed with local law enforcement leaders. "It's not so much administrative dollars and cents; it's the engagement we have with the community," Hartnett said. "The Cleveland law enforcement community has tremendous respect for the way we've professionalized our security operation, that, in many cases, they look at us as almost another law enforcement agency."

Among the key takeaways from JFC Security's experience:

- **Leverage the relationships of your federation's community security Advisor.** JFC Security's strong ties to the Cleveland law enforcement community has enabled it to recruit and hire experienced security professionals, gain real-time insights, and communicate during fast-moving crises, and in some cases, even secure law enforcement resources. For example, thanks to the strong collaborative relationships with a local regional dispatch center, JFC Security has been able to utilize the center's mobile surveillance cameras, originally purchased for the 2016 Republican National Convention, and have them deployed around local synagogues during High Holidays and at large-scale community special events for remote monitoring.

- **Understand the insurance impact of your security decisions.** Pay attention to the direct costs of hiring security officers, but also the indirect costs of the potential liability your organization may be taking on. This is an even larger concern if you decide to rely on armed officers.

- **Thoroughly vet and train your security staff.** Start by relying on local law enforcement connections to identify area police officers and other officials contemplating retirement. Then, make sure that you conduct a comprehensive background check, including psychological, physical fitness, and firearms testing, to ensure their fitness to serve. In addition, JFC Security also requires an annual background check, health assessment, and ongoing tactical firearms training for all armed security professionals.

- **Develop more than just a financial/business relationship with the institutions you serve.** Each Cleveland Jewish institution that receives Federation-subsidized security assistance must sign a formal memorandum of understanding regarding the cost, liability, and nature of the services being provided. Each organization also must agree to strengthen its own security measures, including providing extensive safety and emergency training for their own usher corps and front-line staff, and ensuring that there are access control protocols for locking the institution's doors. This has helped bring up the minimum level of security for the entire Cleveland Jewish community.

- **Scale administrative infrastructure to the size of your program.** As your program grows, you may need to hire more staff, add backroom support, formalize staff evaluations, policies and procedures, institute supervisory oversight, and so on. Be prepared to deal with the management of additional human resources to include administrative policies, tracking of inventory, scheduling hours, ongoing training, uniforms, weapons, radios, vehicle operations, and progressive discipline when necessary.

CREATING A SUSTAINABLE SECURITY PARTNERSHIP

Ultimately, the success of your organization's security program will come down to how well your private security officers are managed. That often falls on the policies and procedures put in place at the time of the RFP and then reassessed each time the contract is renewed. What policies should your organization consider so it can manage the day-to-day relationship most effectively? Below, we review some of the most essential considerations:

KEY CONSIDERATIONS FOR MANAGING YOUR ORGANIZATION'S SECURITY TEAM

Where should security officer staffing levels be set?

Even though every organization has unique security needs, determining the right staffing levels should be largely formulaic. As a rule of thumb, security experts suggest that every 24-hour post requires staffing three separate, eight-hour shifts — or a total of six security officers to provide around-the-clock support each week. It's crucial to get the core staffing levels right because, over time, coverage costs can quickly add up. In addition, you'll need to understand how many consecutive hours your private security provider will allow its contracted officers to work; your organization's leaders should feel comfortable requesting a cap on having too many consecutive hours to ensure the security team is alert and fresh when reporting for duty.

Of course, your organization must also manage its staffing plans for peak periods and special events. For example, in the Jewish community, Shabbat services on Fridays or Saturdays can dramatically increase the number of worshippers entering the synagogue, often at the same time. And High Holiday services can attract many times the number of congregants as on a typical Shabbat. Understanding traffic patterns and event-specific factors, such as whether baggage screening is required, will determine how many additional security professionals your organization may need. For each special event, it's important to draft, review, and revise an operations event plan in consultation with your security company's managers. Delivering a pre-event briefing to local law enforcement is advisable too.

Finally, don't hesitate to contact your organization's security director or tap into the resources of SCN or your local federation or regional security director or Advisor. These experienced professionals can work with your organization and help determine the right staffing resources you need.

What should your organization's security officers wear?

Whether or not to have security officers sport formal uniforms, adopt more casual dress, or be hidden in plainclothes is an important consideration for every organization. There is no right or wrong answer. However, there are some critical trade-offs.

A uniformed security professional will stand out and have a strong, visible presence. Congregants and community members will know to whom they can turn in the event of an emergency, and if armed, the security professional may serve as a deterrent. Security officers in casual dress, such as dress slacks and a knit polo shirt, offer a friendlier and potentially more approachable alternative. If an important goal is community engagement, this may be the ideal style. Finally, a plainclothes security officer will blend into the congregation or broader community. While some community members may be more comfortable, others may feel less secure without a visible uniformed officer. When contemplating uniforms for armed private security officers, there may be additional considerations. For example, whether the officers are legally allowed to conceal their firearm can factor into the decision of dress. Some organizations employ a combination of these choices for both optic and security reasons.

WHAT ARE POST ORDERS?

"Post orders" are detailed instructions to individuals assigned to a specific security post, and they are essential to the effectiveness of the security officer. Most private security companies have templates or standard post orders for the usual and customary types of security posts to which their officers are assigned.

As the contracting organization, it is incumbent on your leadership team to review those standard or templated orders and make sure they are customized to your institution's concerns, expectations, and needs. The post orders should reflect the culture of your organization and its security and other protocols, policies, and procedures. Particular attention should be paid to when and how a security officer should elevate notification, handling, or decision making of any incidents that occur at the post. Post orders should be reviewed, and amended as necessary, after any incidents and as part of periodic reviews of contract performance.

How should your organization manage post orders for its security officers?

Developing post orders, or the basic checklist of expectations that the hiring organization has of its security officers, should be a collaborative process between the security company and the organization it serves. In general, we recommend that the private security company draft post-specific orders for the different positions and roles of the security officers based on input from their client. Organizations should feel free to provide valuable, facility-specific insight into what they want addressed. For Jewish organizations, in particular, there should be specific orders for "normal" operations, as well as those covering Shabbat, other major holidays, and large community events. The organization's security leaders (perhaps through a security subcommittee) should review, revise, and approve all post orders. Finally, once the locations and types of post orders have been approved, your organization's security leaders must identify, in the post orders, who within the organization is authorized to change or update the orders.

For some companies, security officers will be provided a tablet device containing their post orders and other relevant facility information. Some even have software that can track them using RFID and GPS technology to ensure they check certain areas. Remember: Without post orders, there is no accountability. So, if your organization's leaders expect their security officers to be checking a certain facility entrance each hour, it must be in the orders. If not, it's unlikely to be done.

How can your organization most effectively interact with its outside security provider?

It is critical for each organization to establish a single point of contact with its security provider as well as an after-hours contact number. Your organization should identify which staff member or volunteer lay leader is the point of contact for security professionals on a daily basis as well as in the event of an emergency. This person could be the facilities manager, executive director, security subcommittee chair, or someone else with deep knowledge of the organization.

Meanwhile, the private security company should identify which security manager is the point of contact for all security-related issues. This includes training, staffing, scheduling, and feedback. This individual might be an identified supervisor onsite or a security manager offsite.

SHOULD YOUR ORGANIZATION'S SECURITY OFFICERS BE AUTHORIZED TO CARRY FIREARMS?

Our previous white paper, "Firearms and the Faithful," explored one of the most difficult decisions that a congregation or community of faith must make: whether to rely on armed security. It's a choice that should involve multiple decision-makers and stakeholders, including clergy, trustees, board members, and staff members. Working in consultation with Jewish federation officials, including a security director (if one exists in the community) as well as SCN, is strongly recommended.

Decision-makers must be aware of the perception of firearms among community members. In some locations, the presence of firearms may be readily accepted, or even expected. In other places — or even in institutions within the same community — the presence of firearms may be distressing. Given the controversial nature of this issue, this option can easily divide a community of faith if not adequately considered and communicated properly.

Moreover, a community will need to grapple with a host of considerations to minimize disruption, maximize effectiveness, avoid liability, and ensure sustainability. Having a person with a weapon present — other than a member of law enforcement — can have serious legal implications for an institution, and those implications vary greatly from state to state.

Your organization will need to discuss with its security provider its understanding of what licenses will need to be acquired for legal compliance, what level of training will be required, and who shoulders liability in the event someone is harmed by an armed security officer, staff member, or congregant. It will also have to consider the long-term costs; armed security professionals command higher pay, and insurance is substantially more expensive. And once an organization starts using armed security for even a short period, it may imply continuing.

If your organization elects to have armed security, it should carefully review its private security company's use of force policy and training. The private security company must document that it complies with state mandates for armed security. The company must also certify that it has conducted the required use-of-force policy training and identify any civil or criminal actions within the previous five years against itself, staff, or subcontractors resulting from the use of force, and the outcome of those actions.

Of course, armed security officers may have a range of options available other than deadly force. These include nonlethal weapons, such as pepper spray or foam, expandable batons, and electronic control devices. Their use must similarly be vetted with counsel and trained, tested, and drilled regularly. In addition, your organization must require its outside security company to document that it complies with state regulations for less-than-lethal equipment. The contractor must also certify that it has conducted required use-of-force policy training.

How should your organization evaluate its outside private security officers?

In general, your organization's leaders should conduct a quarterly review of its private security officers' performance. As part of that process, they should analyze how often the security team has met its KPIs and, if not, how to remove any outstanding barriers. Beyond hard performance metrics, your organization will want to qualitatively assess emergency protocols, visitor management policies, and access controls in light of the current environment.

Finally, as part of the assessment process, it may be useful to conduct a 360 review of the security team. This would include receiving self-assessments from the security staff, as well as formal reviews from any supervisors and congregation/community leaders. In addition, your organization might consider putting out a survey to community members to offer them an opportunity to provide feedback and acknowledge extraordinary staff. The insights from the survey can help inform your strategic security planning and give your private security officers a clearer path to improvement.

Following any major events, after-action meetings and assessments should be conducted. These documents will also be taken into consideration in evaluating the private security officer's performance in addition to the organization's security strategy as a whole.

MANAGING YOUR SECURITY OFFICERS

There are significant benefits to breaking down the silos between your organization's security professionals and local law enforcement. Information sharing, collaboration, and trust can facilitate more robust protection and a more seamless emergency response — and ultimately strengthen protection for the entire community. So, how can your organization encourage more cooperation?

KEY CONSIDERATIONS FOR CREATING A SUSTAINABLE PARTNERSHIP

Is your organization encouraging its private security officers to introduce themselves?

There's nothing like the "power of hello." Your organization should encourage its security professionals to invite local law enforcement for an introductory meal or tour of the facility. Your organization also might share observations and/or intelligence of suspicious activity. Both strategies can help build trust and facilitate collaboration and information sharing.

Is your organization treating crisis incidents as opportunities?

In addition to always seeking to make friends before needing them, the event of a crisis provides further opportunity to forge stronger relationships with local law enforcement officials. If there is a critical incident, police leaders will often want to connect with the vulnerable community and ask how they can help. Take advantage of the offer, and most importantly, use it as an opportunity to establish relationships before the urgent timing of an incident — and then work to maintain that relationship.

Can you establish regular opportunities for collaboration and joint training between your security officers and local law enforcement?

Your organization's leaders should encourage their security professionals to set up a formal meeting on a quarterly or semiannual basis to review policies and procedures and information-sharing protocols. Even better, establish joint training exercises. That way, everyone has rehearsed the playbook in the event of an emergency.

> **"To facilitate that good working relationship, arrange a meeting between your security officers and local law enforcement officials on a quarterly or semiannual basis to review policies and procedures on how both sides can most effectively interact."**
>
> **Gil Kerlikowske**, Former Commissioner,
> U.S. Customs and Border Protection

THE ROAD TO MORE RIGOROUS SECURITY PROGRAMS

As the Secure Community Network expands its outreach efforts and support to Jewish communities around the country, we have found that our local Jewish federations and other faith-based organizations are increasingly engaging private security service providers to protect their members and facilities, monitor suspicious activity, respond to emergency or crisis events, and address common threats, such as verbal assault and vandalism. We believe that hiring well-trained, professional security officers — and equipping them with the right technology and support infrastructure — is critical to these efforts.

But it's also clear that there is no "right way" of establishing a security program. The needs of any community — and its organizations — are unique, and so are the solutions.

That is why instead of coalescing around a set of formal requirements or standards, this white paper was organized around a series of key questions and considerations that can guide your organization's approach — from initiating a proposal to implementing a program, and then managing it over the long run. While the report provides expert insights at a more granular level, here are eight overarching questions that we feel every organization would be wise to keep in mind:

1. What are our security needs — and how do we align them with our risk profile and financial resources?
2. What are the primary goals of our security program? How will our progress be measured? And how are these objectives reflected in our request for proposal?
3. What specific capabilities, certifications, and training requirements will we establish for our security officers?
4. What is the appropriate level of compensation for our security officers? How do we get the biggest bang for our buck?
5. What choices regarding security technology, firearms, and uniforms are right for our community?
6. How do our choices affect our potential financial or legal liability?
7. What post orders are we giving our security officers? And what technologies or processes do we have in place for ensuring they've been executed?
8. Have we set up the mechanisms to foster close collaboration between our security officers and local law enforcement?

The answers to these questions will undoubtedly be different for every organization and community of faith. But perhaps just as important is the process of considering them. By thinking through these and other challenging questions your organization may have in advance, you will be automatically injecting more rigor into the selection, training, and oversight of the security officers your organization hires — and have a head start on the road to keeping your community safe.

APPENDIX 1: Sample Request for Proposal

A MENU OF POTENTIAL TRAINING OFFERINGS

Operational Training: Foundational Training on Core Aspects of Security
Security Awareness: Basics of how their role fits into the organization's comprehensive security plan
Life Safety: Fundamental fire safety, medical emergency, and evacuation skills
Active Assailant Training: Crisis management training for violent attacks
Situational Awareness: Behavioral awareness and screening tactics
Emergency Response Procedures
Incident Response/Crisis Management
Crisis Intervention (mental health)
Principles of Access Control
Bomb Threat Management
Package Screening
Traffic Control/Crowd Control
Industrial Control System Security (ICS)
Incident Response
Crisis Management
Emergency Operating Procedures
Emergency Responder Coordination
Legal Considerations
Use of Force

Communications Training: Internal and External Communication Protocols
Internal Security Communications Protocols
External Security Communications Protocols
Incident Reporting: Immediate vs. incident reports; daily logs
Communicating With Law Enforcement/911
Customer Service: Interacting with congregants; power of hello, disability awareness

Roles and Professional Guidelines: Other Key Security Topics
Cultural Sensitivity and Competency
Diversity, Equity, and Inclusion/Implicit Bias Training
De-escalation/Conflict Resolution Awareness
Engagement With Law Enforcement
Job Assignment and Post Orders

Additional Considerations for Armed Private Security Officers
Incident Response
Crisis Management
Emergency Operating Procedures
Emergency Responder Coordination
Legal Considerations
Use of Deadly Force
Less Than Lethal Weapons Training
Shoot Don't Shoot Protocols/Scenarios (requirements)
Weapons Training & Qualification (initial)
Firearms Practice: No fewer than two paid range days each year
Police Officer Standards & Training (POST) Qualification Course
Weapons Retention and Manipulation (including recent and regular training on stress-induced shooting)

REQUEST FOR PROPOSAL — SECURITY SERVICES

Advertised: XX DATE
Requestor: INSERT YOUR ORGANIZATION'S NAME HERE
Address: INSERT YOUR ORGANIZATION'S ADDRESS HERE
Submit via email to INSERT YOUR EMAIL HERE
Deadline: Submit proposals by: XX DATE

Article 1. Purpose and Term

1.1 The Organization (Client) is seeking proposals from qualified Contractors with demonstrated experience in the provision of high-quality ARMED or UNARMED security services using fixed post and patrol security officers in accordance with the terms and conditions of this request for proposal (RFP). This RFP establishes the minimum requirements a bidder must meet to be eligible for consideration and does not obligate the Client to accept responses from eligible Contractors.

1.2 The selection of the successful Contractor will be made based on the Client's evaluation of the relative ability of each Bidder to deliver quality service in a cost-effective manner. The Client is not obligated to accept the lowest bid and reserves the right to reject any bids or amend the scope of the project. All Bidders must be duly licensed to and perform work in accordance with all federal, state, and local authorities and to the satisfaction of those authorities.

1.3 The following specific criteria will be evaluated and must be addressed in the proposal:

a) Company history and organization, including experience and depth of organization
b) Demonstrated successful experience in implementing services similar to those requested in this RFP
c) Ability to meet the contractual requirements set forth in this RFP
d) Provisions of other value-added services
e) Process improvement/cost savings ideas presented by Bidder
f) Licensing
g) Safety record
h) Hiring standards for employees
i) Training provided to employees
j) Employee benefits
k) References
l) A statement of the hourly wage rate for the security officer(s), the regular hourly rate billed to the Client for services, a breakdown of the benefits package, overtime wage rates, and related items
m) The proposal's completeness, thoroughness, accuracy, compliance with instructions, timeliness, and conciseness of the text materials.

1.4 Any other criteria that the Client in its reasonable discretion deems applicable to the evaluation of proposals. This shall have an initial term beginning on INSERT TERM START DATE HERE and running through INSERT TERM TERMINATION DATE HERE and shall continue in effect from year to year thereafter, provided, however, that either party may terminate this Agreement at any time upon thirty (30) days prior written notice to the other party

Article 2. Services

2.1 Contractor to provide ARMED or UNARMED security officers at INSERT NAME OF ORGANIZATION, located at INSERT ORGANIZATION ADDRESS. Contractor to provide security protection services during the Organization's operations to include, but not be limited to:

a) Controlling access at all entrances
b) Visitor management including monitoring the visitor invitation system and checking visitors in
c) CCTV and alarm monitoring
d) Patrolling the inside and outside of the building; being visible inside the facility and lobby to greet employees, guests, and congregants
e) Filling the incident commander role during security- and emergency-related incidents when the person at the Organization responsible for security supervision or more senior management is not on-site
f) Communicating via telephone, text, email, and radio using clear, concise language
g) Reviewing existing policies and procedures and providing recommendations to person at the Organization responsible for security supervision
h) Handling other security-related functions as required and agreed upon between the Contractor and the Client
i) Property management system monitoring (HVAC, water, etc.), communicating with the facility manager (or designee) of any abnormalities, and simple troubleshooting under that person's instructions
j) Adhering to all COVID-19–related policies and procedures put in place at the Organization's building or any space in which the Contractor may be working

2.2 Contractor is to provide ARMED or UNARMED security officers at the Organization's building and offsite events in INSERT CITY/TOWN/COUNTY HERE area. The Organization will provide Contractor with written request for services, location, and hours. Contractor will provide ARMED or UNARMED security protection services during the Organization's events to include, but not be limited to, access control at all entrances; visitor management; patrolling the inside and outside of the building; being visible inside the facility and lobby to greet employees and guests, and additional security-related functions as required.

2.3 Hours of service:

a) Weekdays: INSERT REQUIRED HOURS OF SERVICE HERE
b) Saturdays and Sundays: INSERT REQUIRED HOURS OF SERVICE HERE
c) The Organization will advise at least one week in advance when additional services are required for events or High Holidays.
d) The Organization will advise at least one week in advance if services are required on federal or state holidays.

2.4 Contractor shall perform all such tasks as are necessary or incidental to the satisfactory performance of such services within the time frames and whatever other parameters may be established by the Organization and communicated to the contractor.

2.5 Both parties may, at any time, make changes in the services to be performed by the Contractor within the general scope of this Agreement.

2.6 Minimum Acceptable Wage Range:
To ensure that qualified, trained security officers are retained, the Organization requires that a minimum gross hourly wage of INSERT ACCEPTABLE WAGE RANGE HERE be paid to the security officer. When required to work overtime hours or to work on federal or state holidays, security officers must be paid at least 1.5 their normal hourly wage rate. If the Client requests holiday or overtime coverage, the Client will be billed at the overtime rate.

2.7 The Contractor is required to pay security officers at their hourly rate for at least two annual training days for firearm qualifications, physical fitness tests, and other required training. This is in addition to vacation days and sick or medical days as required by law. The training and sick and vacation days will not be invoiced to the Client.

Article 3. Qualifications, Training, Equipment, Uniform

3.1 Required Experience:
Contract security officers must possess at least two years of prior military, law enforcement, or contract security officer experience.

3.2 Annual Training Required:
a) The Contractor must furnish personnel and training records for two permanently assigned and at least one replacement contract security officer within 30 days of contract award.
b) The Contractor must ensure that two permanently assigned and at least one replacement contract security officer receive annual development and refresher training as outlined herein.

3.3 Required Licensing and Training: (Items A and B applicable/important to armed security)
a) Firearms: Contractor security officers must possess valid firearms licenses, hold the appropriate training certificates, and meet INSERT STATE or COMMONWEALTH NAME HERE police firearms qualifications standards (annual basis).
b) "Shoot don't shoot" scenario training (annually).
c) Legal: use-of-force continuum per state guidelines, legal training on contractor security officer roles/responsibilities and legal limitations (annual basis).
d) Client service training, including appropriate interactions with children and individuals with functional and access needs (special needs); diversity training, including, at a minimum, race, gender, religion, and sexual orientation; prevention of sexual harassment.
e) De-escalation training; conflict resolution; and threat-assessment training.
f) Medical: first aid, CPR, "Stop the Bleed" training to Red Cross or AHA standards (annual basis, recertification provided by the Organization).
g) Contractor must determine appropriateness and advise the Organization about any "less than lethal," OC, or other "empty-hand" control techniques training provided, certifications, or standards for such training.
h) All training must comply with relevant state laws, guidelines, or authorizations.
i) Contractor must provide initial and annual training records and applicable certificates to the Client on an annual basis for at least two contractor security officers assigned to the Organization and one replacement within 30 days of contract award.

3.4 Physical Fitness Training Standards:

a) On an annual basis, contractor security officers must complete the U.S. State Department, Diplomatic Security Service, Physical Fitness Test and receive a score of "Good" or above as appropriate for their age and gender. This test requires the satisfactory completion of two minutes of pushups, two minutes of situps, and a 1.5-mile run — all completed within 45 minutes (see Appendix 2).
b) The Contractor must provide consistent personnel and give the Client advanced notification of any changes to assigned personnel.
c) The Contractor will provide up to eight additional personnel at the same hourly cost as indicated for regular security services in the case of an emergency or scheduled event.
d) The Client will provide the Contractor with one week's advance notice for event scheduling and at least 24 hours' advance notice to request additional personnel for scheduled events.
e) The Contractor will establish and/or revise post orders and training standards that are preapproved by the Client and make changes as needed and/or directed by the Client (initiation upon award of contract, completion within 90 days of contract award).

3.5 Equipment: (Items A, B, and C applicable/important to armed security)

a) Legally licensed registered semiautomatic firearm in the state
b) Concealed retention holster
c) Two spare magazines complying with state standards
d) Two-way radios for communication between contractor security officers and Organization staff. Contractor must provide ear pieces to each assigned security officer.

3.6 Daily Uniform/Dress Code:

a) Collared button-down white or blue shirt (ironed)
b) White undershirt
c) Blazer: Dark blue or black — must fully conceal firearm
d) Pressed dress pants: khaki, black, dark blue, dark brown, dark gray
e) Black dress shoes, rubber soles, and reinforced black dress belt constructed for firearm and magazines OR dark brown dress shoes, rubber soles, and reinforced brown dress belt constructed for firearm and magazines

3.7 Casual Uniform/Dress Code:

Upon contract award, Contractor will propose a casual dress code for training days, Client-specified outdoor events where the Client determines formal attire inappropriate, Client-specified after-hours construction or cleaning days. Casual dress code might include khakis, dark polo shirts, and appropriate jacket to conceal firearms and related equipment.

Article 4. Schedule of Events, Instructions to Bidders, Contractor Company/Organization-Required Qualifications

4.1 Schedule of Events:

1. RFP Issue — XX Date
2. Acknowledgment Expression of Interest:
   Detailed Proposals Due — XX Date (30 days after #1)
3. Question Deadline — XX Date (30 days after # 1)

4. Award — XX Date (30 to 60 days after # 2)
5. Contract Commences — (30 to 60 days after # 4)

4.2 Contact with Client Staff, Representatives, and/or Agents:
Direct contact with Client staff, representatives, and/or agents is expressly prohibited except as outlined in 4.3.

4.3 Questions and Addenda:
Bidders shall carefully examine this RFP and any addenda. Bidders are responsible for seeking clarifications of any ambiguity, conflict, omission, or other errors in this RFP in writing. Questions shall be addressed to INSERT EMAIL ADDRESS(ES) HERE. If the answer materially affects this RFP, the information will be distributed to any Bidder who expressed interest. Oral comments and/or instructions do not form a part of this RFP.

4.4 RFP Terms and Conditions Applied to the Contract:
This document is a request for proposals for Client comparison and evaluation. A final contract would incorporate elements of the RFP and any modifications in writing and would be reviewed and executed by both parties.

4.5 Nondiscrimination and Equal Employment:
The Client is committed to equal employment opportunity. The Client expects that the Contractor will ensure persons are recruited, hired, assigned, and promoted without regard to race, religion, color, national origin, citizenship, sex, sexual orientation, gender identity, veteran status, uniform service member status, age, disability, or any other legally recognized protected personal characteristics.

Similarly, all other personnel actions, such as compensation, benefits, transfers, layoffs and recall from layoffs, access to training, education, tuition assistance, and social recreation programs must be administered without regard to race, religion, color, veteran status, uniform service member status, national origin, citizenship, sex, sexual orientation, gender identity, age, disability, or any other legally recognized protected personal characteristics.

4.6 Compliance with Federal Immigration Law:
The Contractor must certify that, at all times during which any term of a contract resulting from this solicitation, it does not and shall not knowingly employ any unauthorized alien. For purposes of this section, an "unauthorized alien" shall mean any alien who is neither lawfully admitted for permanent residence in the United States nor authorized to be employed by either Title 8, section 1324a of the United States Code, or the U.S. Attorney General.

4.7 Authorization to Transact Business in INSERT CITY or COUNTY AND STATE:
The Contractor shall provide proof that it is organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a limited liability partnership and is authorized to transact business in the INSERT STATE HERE.

4.8 Criminal Background Check and Drug-Free Workplace:
All contract security officers must complete a satisfactory fingerprint and background check that includes multistate criminal as well as sex offender (CORI) status on an initial and annual basis. For contract security officers domiciled

in INSERT STATE HERE, the background investigation must include records checks with courts that do not provide electronic records in the areas where the contractors have lived in the preceding five years. The Contractor will conduct the investigation prior to assigning personnel to the account and agrees to make the results available to the Client within 30 days of contract award. The Contractor will also conduct an open-source social media review of contract security officers on an initial and annual basis. The Contractor will notify the Client of any legal actions or change of employment (suspension, termination, etc.). The Contractor will ensure that all contract employees assigned to the account will maintain their status while employed on Client property. All contract employees who operate or have access to a vehicle must have a valid driver's license in their state of residence.

4.9 During the performance of this Contract, the Contractor agrees to provide a drug-free workplace for the contract employees. A drug-free workplace means contract employees are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession, or use of any controlled substance — including marijuana and related substances — during the performance of this Contract. The Contractor agrees to drug test contract employees prior to permanent assignment to the Contract, randomly drug test contract employees, at the Client's request, and after any contract employee accident or negligent action.

4.9.1 Cost Incurred in Responding:
This RFP does not commit the Client to pay any costs incurred in the preparation and submission of proposals or in making necessary studies or designs for the preparation thereof, nor to procure or contract for services.

4.9.2 Right of Refusal:
The Client has the right to refuse any assigned personnel at any time. The Contractor will replace the personnel with qualified, trained personnel within 24 hours of notification by the Client.

4.9.3 Disposition of Proposals:
On receipt by the Client, all materials submitted in response to this RFP will become the property of the Client. One (1) copy of each proposal shall be retained for official files.

Article 5. Required Insurance (Review insurance levels with insurer)

5.1 Contractor shall procure and maintain at its own expense during the term of this Agreement the following insurance coverage:

COVERAGE	LIMITS
a. Workers' Compensation	Statutory
b. Employer's Liability	$1,000,000
c. General Commercial Liability	$1 million each occurrence $3 million aggregate
d. Automobile	$1 million combined single limit

The Client must also be listed as an Additional Insured on the General Liability, Auto, Professional, and Umbrella policies. The Client reserves the right to request additional or revised Contractor insurance information based on review and recommendation by the Client's insurance provider.

5.2 The above-mentioned Workers' Compensation, Automobile Liability, and General Liability and Umbrella insurance policies shall contain a waiver of subrogation in favor of any Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property that may arise from or be in connection with the performance of the work hereunder by the Contractor, their agents, representatives, or employees. If the Contractor maintains broader coverage and/or higher limits than the minimums shown below, the Organization shall be entitled to the broader coverage and/or higher limits maintained by the Contractor.

Contractor agrees, at its sole cost and expense, to procure and maintain in full force and continuous effect at all times during the term of this Agreement and the performance of services by contract employees, insurance for itself and its employees, with insurance companies authorized to do business in the state(s) where work is to be performed, covering all operations under this Agreement, of the following types and/or kinds of coverage and maintaining the following minimum policy limits:

a) Workers' compensation insurance as prescribed by the law of the state(s) in which the work is performed, including Employer's Liability insurance with limits of at least one million dollars ($1,000,000) for each occurrence will apply.

b) Automobile Liability insurance with limits of at least one million dollars ($1,000,000) combined single limit for bodily injury and property damage for each occurrence, covering all hired and non-owned vehicles, and, only in the event that Contractor owns vehicles, covering owned autos as well.

c) General Liability insurance, including Blanket Contractual Liability covering the indemnity provisions of this Agreement, with limits of at least three million dollars ($3,000,000) each occurrence for bodily injury, personal injury (e.g. slander, libel, wrongful detention, false arrest) and property damage for each occurrence and Employers Liability Stop Gap Coverage, where applicable. If Commercial General Liability Insurance or other form with a general aggregate limit is used, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.

d) Employee Dishonesty Coverage under a Crime Policy or Fidelity Bond, with limits of at least one million dollars ($1,000,000) for each occurrence.

e) Professional Liability insurance, with a minimum $1,000,000 limit for each wrongful act and aggregate of not less than $3,000,000, including an extended reporting period endorsement ("tail policy") for the term of three years in the amount of not less than $1,000,000 per claim if professional services are being rendered.

f) Umbrella Liability coverage with a minimum of not less than $5,000,000.

5.3 The above-mentioned Workers' Compensation, Automobile Liability, and General Liability and Umbrella insurance policies shall contain a waiver of subrogation in favor of the Organization, their respective directors, officers, employees, and volunteers as to all applicable coverage(s). The Automobile Liability, General

Liability and Umbrella insurance policies shall cover Contractor employees assigned to work for the Client and must provide for the Organization to be named as additional insured on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of t he Contractor including materials, parts, or equipment furnished in connection with such work or operations. The Organization must be primary and noncontributing, and Contractor's policy is required to respond and pay prior to any other available coverage. The limits required for Automobile Liability and General Liability insurance may be satisfied with any combination of primary and umbrella or excess liability policies.

5.4 If any of the required policies provide claims-made coverage:

a) The retroactive date must be shown and must be before the date of the contract or the beginning of contract work.
b) Insurance must be maintained, and evidence of insurance must be provided for at least five (5) years after completion of the contract of work.
c) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, the Consultant must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

5.5 Prior to the commencement of work under this Agreement, Contractor shall provide to the Organization certificate(s) of insurance from insurance companies acceptable to the Organization evidencing such coverages as mentioned above. Contractor shall notify the Organization thirty (30) days prior to any material change in coverage during the term of this Agreement.

5.5.1 Should any insurance policy the Contractor is required to maintain under this Agreement expire or be canceled before completion of the services or work, or termination of this Agreement, and Contractor fails to immediately procure replacement insurance as required, the Organization reserves the right (but do not have an obligation) to procure such insurance and to deduct the cost thereof from any sum due to Contractor under this Agreement. The Organization exercise of its right under this provision shall not in any way limit its right to demand performance by Contractor or to demand any other remedy provided for or permitted under this Agreement.

5.5.2 Upon award of the contract and thereafter on an annual basis, the Contractor must furnish certificates to the Client prior to contract renewal and/or upon request.

5.6 Confidentiality:
All contract employees shall maintain confidentiality while on or off the property. "Confidential information" shall mean all nonpublic information of the Client or its affiliates, subsidiaries, customers, clients, vendors, and contractors (whether oral, written, or electronic), including any analyses, compilations, studies, notes, or other documents that contain or otherwise reflect such information. Confidential information includes but is not limited to financial, commercial, human resource sensitive, and technical data, analysis and information; strategies, projections, forecasts, assumptions, and results; inventory; procurement practices; customer, supplier, vendor, contractor and pricing lists and information; management structure and organizational needs; methods of production, distribution, or operation; technology in any stage of development, trade secrets, techniques,

processes, concepts, ideas, inventions, know-how, and all copies, compilations, and derivative works thereof and any visual observations or conversations overheard by the Contractor or its Employees. Every contract employee must sign a confidentiality agreement provided by the Contractor, with prior approval of the Client, prior to employment.

5.7 Indemnification:
The Contractor shall indemnify and hold harmless the Client and its representatives from and against all losses and claims, demands, suits, actions, payments, and judgments arising from personal injury or otherwise, brought or recovered against the Client and its representative by reason of any act, negligence, or omission of the Contractor, its agents, or employees, in the execution of the contracted work, including any and all expense, legal and otherwise, incurred by the Client or its representatives in the defense of claim or suit.

5.8 Should any insurance policy the Contractor is required to maintain under this Agreement expire or be canceled before completion of the services or work, or termination of this Agreement, and the Contractor fails to immediately procure replacement insurance as required, the Organization reserves the right (but does not have an obligation) to procure such insurance and to deduct the cost thereof from any sum due to the Contractor under this Agreement. The Organization's exercise of its right under this provision shall not in any way limit its right to demand performance by the Contractor or to demand any other remedy provided for or permitted under this Agreement.

5.9 Upon award of contract and thereafter on an annual basis, the Contractor must furnish certificates to the Client prior to contract renewal and/or upon request.

5.10 Confidentiality:
All Contract Employees shall maintain confidentiality while on or off the property. "Confidential information" shall mean all nonpublic information of the Client or its affiliates, subsidiaries, customers, clients, vendors, and contractors (whether oral, written or electronic), including any analyses, compilations, studies, notes, or other documents which contain or otherwise reflect such information. Confidential Information includes but is not limited to financial, commercial, human resource sensitive, and technical data, analysis and information; strategies, projections, forecasts, assumptions and results; inventory; procurement practices; customer, supplier, vendor, contractor and pricing lists and information; management structure and organizational needs; methods of production, distribution, or operation; technology in any stage of development, trade secrets, techniques, processes, concepts, ideas, inventions, know-how, and all copies, compilations, and derivative works thereof and any visual observations or conversations overheard by the Contractor or its Employees. Every contract employee must sign a confidentiality agreement provided by the Contractor, with prior approval of the Client, prior to employment.

APPENDIX 2: Physical Readiness Testing

Diplomatic Security
Physical Readiness Test (PRT) Testing Protocol

Event Order:
- Pushups
- Situps
- 1.5-Mile Run

Break Between Events:
No less than two minutes and no greater than 15 minutes of rest (to include movement between test sites).

Pushups:
Pushups shall be performed on a firm or suitably padded, level surface. Shoes are optional.

Pushups shall be performed as follows:
- Participant shall begin in the high plank position, palms or fists placed on floor directly beneath or slightly wider than shoulders. Both feet together on floor. Crossing at the ankles is NOT allowed.
- Back, buttocks, and legs shall be straight from head to heels and must remain so throughout test. Toes and palms/fists shall remain in contact with floor. Feet shall not contact a wall or other vertical support surface.
- The test proctor shall signal start for participants and call out 15-second time intervals until two minutes have elapsed.
- Participants shall lower themselves while maintaining the bodily alignment so that the chest (men)/ chin (women) makes contact with a counter's fist. Minimum height of the fist or object used to substitute shall be 3". Males will touch chest to fist. Females will touch chin to fist.
- Participants shall return to starting position by extending elbows, raising the body while maintaining a plank until arms are at a near lockout.
- Participants may rest only in the up position while maintaining arms, back, buttocks, and legs in straight position. Participants may briefly move into an arch to stretch out but must move into a full plank position before resuming movement.
- Pushups are repeated correctly as many times as possible in two minutes. Proctors are to monitor participants for correct form and count correctly performed pushups.
- Incorrect pushups shall not be counted. If the event ends in less than two minutes, the results shall be the number of pushups properly performed at time of termination.

Event is ended if participant:
- Touches deck with any part of body except hands and feet.
- Raises one or both feet or hands off deck or ground.
- Fails to maintain back, buttocks, and legs straight from head to heels during execution of the movement.

Situps:
Event shall be conducted with partner on a level surface on a blanket, mat, or other suitable padding. Shoes are optional.

Situps are conducted as follows:
- Participants shall start by lying flat on back with knees bent, heels about 10 inches from buttocks. Arms shall be folded across and touching chest with hands touching upper chest, shoulders, or upper arms.
- Feet shall be anchored to floor only by having a partner anchor with hands, knees, or sitting upon the feet of the participant.
- Proctor shall signal start for participants and call out 15-second time intervals until two minutes have elapsed.
- Participants curl their body up, touching elbows to the bottom of thighs while keeping hands in contact with chest, shoulders, or upper arms.
- After touching elbows to the bottom of the thighs, participants lie back, touching the small of the back to the ground. Participants may touch shoulders without penalty.
- Participants may rest in the down position. There is no time limit to length of rest other than the time limit of the test itself.
- Situps are repeated correctly as many times as possible in two minutes. Proctors monitor participants for correct form and count number of correctly performed situps.
- Incorrectly performed situps shall not be counted. Results for event ended in less than two minutes shall be the number of situps properly completed at time of test termination.

Event is ended if participant:
- Lowers legs.
- Raises feet off ground or floor.
- Lifts buttocks off ground or floor .
- Fails to keep arms folded across and touching chest/shoulders/upper arms.

1.5-Mile Run:
Event shall be conducted on a track or outdoor course with a reasonably flat surface as designated by testing staff.

The 1.5-Mile Run Event shall be conducted as follows:
- Participants shall stand at start line.
- Test proctor shall signal start and call out time intervals until completion of test at either the split of the events distance or per lap depending upon course used.
- Time is recorded with stopwatch to nearest second.

The 1.5-Mile Run Event shall be conducted on a treadmill as follows:
- Participants straddle treadmill belt with treadmill inclination set to 1.0 percent.
- Test proctor shall signal start, and participants start treadmill at desired speed.
- Proctor calls out time intervals every .25 mile until completion of test.
- Time is recorded with stopwatch to nearest second.
- Treadmill speed may be adjusted to each participant's comfort anytime during test. Only the participant may adjust treadmill speed unless there is a threat to the health of the participant.
- Touching bar with fingertips or open palm for safety to recover balance is acceptable.

Event is ended if participant:
- Stops running or walking other than to retie shoelace or remove foreign object from shoe.
- Completes 1.5 miles.
- Changes treadmill inclination from 1.0 percent.
- Supports body weight using arms, hands, torso, or any mechanical device.

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 20 TO 24 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	105	87	8:30
Outstanding	95	103	86	9:00
Excellent	90	98	81	9:15
Excellent	85	94	77	9:45
Very Good	80	90	74	10:00
Good	75	87	71	10:30
Good	70	78	64	10:45

FEMALES: AGE 20 to 24 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	105	48	9:47
Outstanding	95	103	47	11:15
Excellent	90	98	44	11:30
Excellent	85	94	43	12:15
Very Good	80	90	40	12:45
Good	75	87	39	13:15
Good	70	78	33	13:30

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 25 TO 29 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	101	84	8:55
Outstanding	95	100	82	9:23
Excellent	90	95	77	9:38
Excellent	85	91	73	10:15
Very Good	80	87	69	10:30
Good	75	84	67	10:52
Good	70 7	5	60	11:23

FEMALES: AGE 25 to 29 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	101	46	10:17
Outstanding	95	100	45	11:30
Excellent	90	95	43	11:45
Excellent	85	91	41	12:30
Very Good	80	87	39	13:00
Good	75	84	37	13:23
Good	70	75	30	14:00

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 30 TO 34 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	98	80	9:20
Outstanding	95	97	78	9:45
Excellent	90	92	74	10:00
Excellent	85	88	69	10:30
Very Good	80	85	67	11:00
Good	75	81	64	11:15
Good	70	73	57	12:00

FEMALES: AGE 30 to 34 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	98	44	10:46
Outstanding	95	97	43	11:45
Excellent	90	92	41	12:00
Excellent	85	88	39	12:45
Very Good	80	85	37	13:15
Good	75	81	35	13:30
Good	70	73	28	14:30

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 35 TO 39 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	95	76	9:25
Outstanding	95	93	74	9:53
Excellent	90	88	70	10:08
Excellent	85	85	65	10:38
Very Good	80	83	63	11:08
Good	75	78	60	11:23
Good	70	70	53	12:23

FEMALES: AGE 35 to 39 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	95	43	10:51
Outstanding	95	93	42	11:53
Excellent	90	88	39	12:08
Excellent	85	85	37	12:53
Very Good	80	83	35	13:23
Good	75	78	34	13:45
Good	70	70	26	14:38

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 40 TO 44 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	92	72	9:30
Outstanding	95	90	70	10:00
Excellent	90	85	67	10:15
Excellent	85	83	61	10:45
Very Good	80	80	59	11:15
Good	75	76	56	11:45
Good	70	68	50	12:45

FEMALES: AGE 40 to 44 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	92	41	10:56
Outstanding	95	90	40	12:00
Excellent	90	85	37	12:15
Excellent	85	83	35	13:00
Very Good	80	80	33	13:30
Good	75	76	32	14:00
Good	70	68	24	14:45

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 45 to 49 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	88	68	9:33
Outstanding	95	86	66	10:08
Excellent	90	81	63	10:30
Excellent	85	80	57	11:08
Very Good	80	78	54	11:38
Good	75	73	52	12:08
Good	70	65	46	13:00

FEMALES: AGE 45 to 49 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	88	40	10:58
Outstanding	95	86	39	12:08
Excellent	90	81	35	12:30
Excellent	85	80	33	13:15
Very Good	80	78	32	13:45
Good	75	73	30	14:08
Good	70	65	22	15:00

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 50 TO 54 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	85	64	9:35
Outstanding	95	84	62	10:15
Excellent	90	78	59	10:45
Excellent	85	77	53	11:30
Very Good	80	76	51	12:00
Good	75	71	49	12:30
Good	70	63	43	13:15

FEMALES: AGE 50 TO 54 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	10	85	38	11:00
Outstanding	95	84	37	12:15
Excellent	90	78	33	12:45
Excellent	85	77	31	13:30
Very Good	80	76	30	14:00
Good	75	71	28	14:15
Good	70	63	20	15:15

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 55 TO 59 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	81	60	10:42
Outstanding	95	80	59	11:09
Excellent	90	74	56	11:25
Excellent	85	70	52	11:57
Very Good	80	66	48	12:29
Good	75	62	46	13:12
Good	70	54	38	14:13

FEMALES: AGE 55 TO 59 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	81	30	12:23
Outstanding	95	80	28	13:39
Excellent	90	74	26	13:57
Excellent	85	70	24	14:25
Very Good	80	66	22	14:53
Good	75	62	20	15:20
Good	70	54	16	16:09

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 60 TO 64 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	75	57	11:21
Outstanding	95	74	56	11:48
Excellent	90	70	52	12:04
Excellent	85	66	48	12:40
Very Good	80	62	46	13:16
Good	75	56	44	13:53
Good	70	40	32	15:00

FEMALES: AGE 60 TO 64 YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	75	26	13:34
Outstanding	95	74	24	14:50
Excellent	90	70	22	15:08
Excellent	85	66	20	15:34
Very Good	80	62	18	16:00
Good	75	56	16	16:25
Good	70	40	12	17:17

AGE/GENDER PRT STANDARDS

At Sea Level (< 5,000')

MALES: AGE 65+ YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	65	48	11:41
Outstanding	95	64	46	12:13
Excellent	90	60	44	12:43
Excellent	85	55	41	13:20
Very Good	80	50	39	13:57
Good	75	44	36	14:34
Good	70	36	25	15:47

FEMALES: AGE 65+ YEARS

Performance Category	%	2 minute SITUPS	2 minute PUSHUPS	1.5-MILE RUN
Outstanding	100	65	22	14:45
Outstanding	95	64	20	16:01
Excellent	90	60	18	16:19
Excellent	85	55	16	16:43
Very Good	80	50	14	17:07
Good	75	44	12	17:30
Good	70	36	9	18:18

APPENDIX 3: Standard Procedures

SAMPLE POST ORDERS

Following situations:

When conducting interior patrols, be on the lookout for:
- Employees or visitors without an ID displayed
- Unauthorized individuals
- Evidence of vagrants in stairwells
- Water leaks and slip/trip hazards
- Inoperable or hard-to-open doors
- Blocked fire exits, fire doors, and fire hazards
- Unattended wallets or purses
- Unattended proprietary information
- Suspicious behavior or activity
- Unsecured offices
- Smoking in stairwells or other inside areas
- Defective cameras or alarm equipment
- Laptops and other unsecured equipment

When conducting exterior patrols, be on the lookout for:
- Broken glass or spilled fluid under or between vehicles
- Suspicious activity or vehicles parked overnight
- Burned-out lighting and inoperable gates
- Openings in gates or fencing
- Illegally parked vehicles
- Loitering
- Stray or wild animals
- Unidentified individuals on roof
- Parking lot/road/sidewalk defects
- Blocked sewers causing water to flood or stand
- Inclement weather: ice, large puddles of water, etc.
- Unauthorized individuals taking photographs of buildings

EMERGENCY RESPONSE PROCEDURES

All security officers must follow a basic emergency action plan. This basic plan can be used for all types of emergencies, from a leaking water pipe in the ceiling to a catastrophic event such as a large fire or a medical emergency. This plan is to be used as the initial response to all emergencies and should be used in conjunction with the facility's emergency/disaster continuity plans.

To keep the basic emergency response plan simple, remember the acronym CAR: Check, Alert, and Response.

Check:
Never enter an emergency location without first observing the area. During this initial observation, the officer must look for anything that might be hazardous or may cause injury to others and/or themselves. Hazardous situations would include fire, smoke, downed electrical wires, machinery operating in the area, traffic, toxic fumes, and so on. The officer's personal safety comes first in all emergencies. An escape route needs to be thought of as the officer approaches the event. Security officers can get themselves into trouble by not thinking about how to get out of the area if the scene becomes unsafe. Thoroughly observing the scene may give the officer insight on what response is needed by the security department as well as additional departments and EMS.

For example:
A security officer is dispatched to a medical emergency where a person is lying on the ground and is unconscious. As the officer approaches the person, the officer sees a ladder lying on the ground next to the person. Based on the information, the officer can assume that the person fell from the ladder and has sustained a head, neck, or back injury.

The security officer should see if there are any bystanders that could be of assistance. They can call 911 or tell the responding officers what has happened. Bystanders can also help keep other bystanders away from the incident.

Alert:
One of the main functions the security department performs is to notify local public safety officials about incidents. The most important point in reporting an emergency is to provide the information that will get help to the victim the fastest.

When placing a call for assistance from public safety officials, the security officer needs to give the following information:

- Their name
- The account company name
- The address including cross streets
- The nature of the assistance needed
- Details of what is happening
- What action is being taken by security/building management
- Where in the building the public safety officials need to go and if they are going to be met by security

The security officer should never hang up with the dispatcher until the operator determines the call is complete. If the dispatcher has further questions, they may want the security officer to stay on the line until officials arrive on-site. If further information has become available and the dispatcher has already disconnected, the security officer should not hesitate in making a second call to update the dispatchers. In addition, some towns' 911 operators have been trained to provide emergency medical care advice to the person calling 911. If an officer is not trained in first aid and the dispatcher can give advice, the officer should attempt to bring the telephone to the victim and follow the advice given.

The security professional's call to 911 will ensure that the proper emergency response entity will be en route to the location quickly. By placing a detailed 911 call, the security officer can assist the dispatcher ascertain what kind of equipment and response are needed.

When calling 911 from a workplace, some companies have a PBX telephone system that allows a person direct access to an outside line on all 911 calls. If the company does not have this type of system, the officer placing the call will need to dial 9-911 (or whatever the number to access an outside line is plus 911). The other option is to call from the post cell phone or a personal cell phone by simply dialing 911.

Response:

The response to an emergency greatly depends on the nature of the emergency. The response can be as simple as placing a bucket under a water leak, to evacuating the building, to providing first responder care and calling 911 for a medical emergency. For a proper response to an event, the officer needs to be aware of the building and the site emergency procedures located in the post order manual.

A security officer has a duty to act when they are working. This means that at any time during an officer's shift, they may be required to respond to emergencies. A Duty to Act during emergencies at clients' facilities is one of the reasons that officers are not allowed to leave the site during their assigned shifts.

MEDICAL EMERGENCY

Responding to a medical emergency may be one of the most stressful situations a security officer will face. The way each officer responds may affect the outcome of the medical emergency. It is imperative that each officer perform their assigned duty as calmly as possible. An excited officer will impede the team effort to resolve the medical emergency and can cause undue stress on the victim.

Noncertified Officer's Response:

In the event there is a medical emergency in the facility or on the property, an officer should be dispatched to the scene of the incident. The responding officer should be sure to write down all the information received about the situation from associates in the area who may be witnesses so it can be relayed to the emergency services personnel. The responding officer should call for an ambulance (911) and explain that there is a medical emergency at the facility. When the security officer is not certified in first aid and/or CPR/AED, they should follow an "observe and report" role. The officer should provide comfort as possible but not exceed their level of training.

Certified Officer's Response:

When responding to a medical emergency, the security officer who is trained and certified in first aid/CPR and AED must follow the guidelines listed below:

- Upon receiving notification of a medical emergency, the officer will immediately retrieve the Medical Emergency Jump Kit (first aid kit) if available and respond quickly to the emergency. (The officer will walk, not run, to avoid becoming another casualty.)
- Upon arriving at the location, the officer will notify the control room officer via radio that

they are on-site. Or, if there is no control room, the officer will notify the supervisor or other on-duty officers if available.

- The officer will don personal protective equipment, such as disposable gloves.
- The officer will check the area to make sure it is safe to help the victim. Then, the officer will check the condition of the victim and what has happened to the victim, including checking for any life-threatening conditions and consciousness.
- If the victim appears unresponsive, the responding officer must do the following:
  - Tap the victim's shoulders and shout, "Are you OK?"
  - If the victim does not respond, inform the control room or supervisor or other on-duty officer(s) if available. Verify that EMS is on the way.
  - Check for breathing. The victim is not to be moved at this time. Ensure the victim is breathing by looking, listening, and feeling for breathing.
  - If it is not possible to tell if the victim is breathing, gently roll the victim onto their back while supporting the victim's neck and head.
  - Tilt the head back and open the jaw. Again look, listen, and feel for breathing.
  - If the victim is not breathing, give two rescue breaths. If the breaths do not go in, follow training on unconscious choking.
  - If the breaths go in, check for victim's response. If there is a response, but no breathing, follow training on rescue breathing.
  - If there is no response, follow training on CPR.
  - If the victim is breathing and has a pulse, check the victim from head to toe for signs of injury.
  - Monitor the victim and await EMS arrival.
- If the victim is responsive, the responding officer must do the following:
  - Before any care can be given, consent must be obtained from the victim.
  - Follow training on checking a conscious victim.
  - Follow training on injuries or sudden illness.
- Keep the control room officer, supervisor, or other on-duty officer(s), if available, updated via the radio. The responding officer or another officer/supervisor will update EMS as necessary.
- Assist with EMS when they arrive on-site.
- Write and file an incident report.

ACTIVE THREAT

Profile of an Active Threat:

An active threat/active assailant is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, an active threat uses firearms(s), and there is no pattern or method to the selection of victims.

Active threat situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims.

Because active threat situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active threat situation.

Good practices for coping with an active threat situation:

- Be aware of the environment and any possible dangers.
- Take note of the two nearest exits in any facility you visit.
- If you are in an office, stay there and secure the door.
- If you are in a hallway, get into a room and secure the door.
- As a last resort, attempt to take the active threat down. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate the shooter.

CALL 911 WHEN IT IS SAFE TO DO SO!

How to Respond When an Active Threat Is in the Vicinity:

Quickly determine the most reasonable way to protect one's own life. Remember that customers and clients are likely to follow the lead of employees and managers during an active threat situation.

- *Run* - If there is an accessible escape path, attempt to evacuate the premises. Those caught in this situation should be sure to:
  - Have an escape route and plan in mind
  - Evacuate regardless of whether others agree to follow
  - Leave belongings behind
  - Help others escape, if possible
  - Prevent individuals from entering an area where the active threat may be
  - Keep hands visible
  - Follow the instructions of any police officers
  - Do not attempt to move wounded people
  - Call 911 when safe to do so

- *Hide* - If evacuation is not possible, everyone should find a place to hide where the active threat is less likely to find anyone. A hiding place should:
  - Be out of the active threat's view
  - Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
  - Not trap you or restrict your options for movement

  To prevent an active threat from entering a hiding place:
  - Lock the door
  - Blockade the door with heavy furniture

  If the active threat is nearby:
  - Lock the door
  - Silence a cell phone and/or pager and turn off any source of noise (i.e., radios, televisions)
  - Hide behind large items (e.g., cabinets, desks)
  - Remain quiet

  If evacuation and hiding out are not possible:
  - Remain calm
  - Dial 911, if possible, to alert police to the active threat's location

  - If you cannot speak, leave the line open and allow the dispatcher to listen

- *Fight* - Take action against the active threat as a last resort, and only when your life is in imminent danger. Attempt to disrupt and/or incapacitate the active threat by:
  - Acting as aggressively as possible against them
  - Throwing items and improvising weapons
  - Yelling
  - Committing to your actions

How to Respond When Law Enforcement Arrives:

Law enforcement's purpose is to stop the active threat as soon as possible. Officers will proceed directly to the area in which the last shots were heard.

- Officers usually form teams of four (4)
- Officers may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment
- Officers may be armed with rifles, shotguns, or handguns
- Officers may use pepper spray or tear gas to control the situation
- Officers may shout commands or push individuals to the ground for their safety

How to react when law enforcement arrives:

- Remain calm, and follow officers' instructions
- Put down any items in your hands (i.e., bags, jackets)
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming, and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

Information to provide to law enforcement or 911 operator:

- Location of the active threat
- Number of shooters, if more than one
- Physical description of shooter(s)
- Number and type of weapons held by the shooter(s)
- Number of potential victims at the location

The first officers to arrive to the scene will not stop to help injured persons. Expect rescue teams composed of additional officers and emergency medical personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once people have reached a safe location or an assembly point, they will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave until law enforcement authorities have given instructions to do so.

Security offers should be prepared to write an incident report.

HAZARDOUS MATERIAL (HAZMAT)

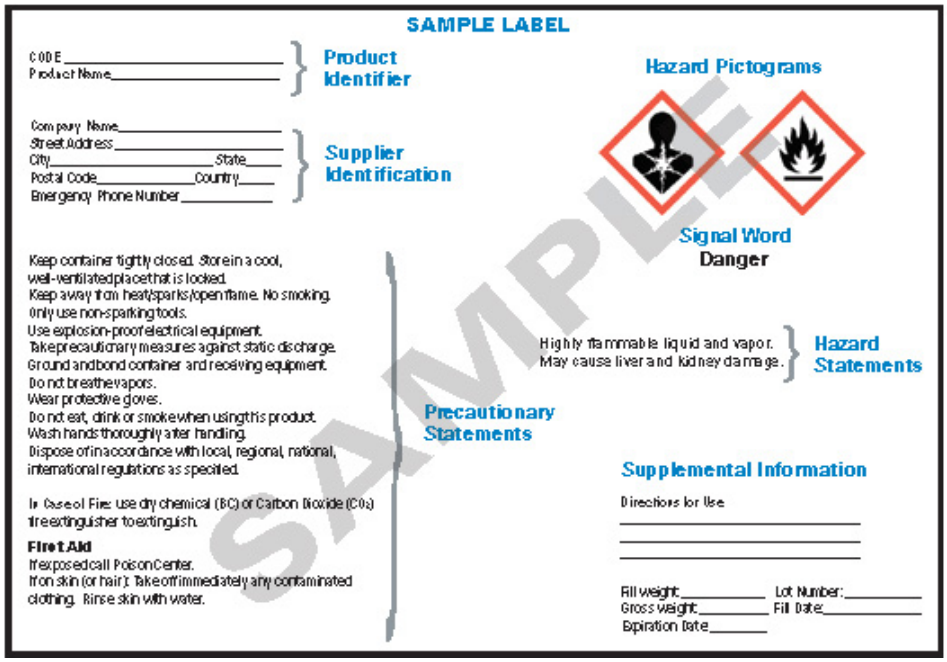
Security personnel play an integral part in emergency response efforts because they may be the first to discover and take action upon an emergency release of hazardous substances. Those security personnel expected to take on an emergency response role must be familiar with the potential hazardous substance releases and emergency incidents to which they may be exposed. To play a key role in communicating the existence of an emergency release, security officers must be well versed in emergency alerting and communication procedures, including whom to contact according to their emergency response plan. A well-trained security staff can help to ensure the proper evacuation of employees and the public, the quick response of an emergency response team, and the proper handling of bystanders and representatives of the media.

Hazard Communication Standard:

In 2012 OSHA revised its hazard communication standard to include the use of the Globally Harmonized System of chemical labeling, identification, and notification. Under this revised standard:

- GHS = Globally Harmonized System of Classification and Labeling of Chemicals
- Mandated in 1992 (UNCED)
- Common and coherent global approach
- Definitions
- Hazard classifications
- Consistent communication on labels and safety data sheets
- Move from Hazard Determination to Hazard Classification
- Reclassifies physical, health, and environmental standards to new GHS standard
- Tiered approach for classification used with chemicals involving mixtures
- Combustible dusts are now included in the revised standard as a hazardous chemical

Labeling Requirements:



GHS Hazard Categories, Signal Words, and Hazard Statements				
Category	**Category 1**	**Category 2**	**Category 3**	**Category 4**
Signal Word	Danger	Danger	Warning	Warning
Hazard Statement	Extremely Flammable	Highly Flammable	Flammable	Combustible

Pictograms and Hazards:

Health Hazard • Carcinogen • Mutagenicity • Reproductive Toxicity • Respiratory Sensitizer • Target Organ Toxicity • Aspiration Toxicity	**Flame** • Flammables • Pyrophorics • Self-Heating • Emits Flammable Gas • Self-Reactives • Organic Peroxides	**Exclamation Mark** • Irritant (skin and eye) • Skin Sensitizer • Acute Toxicity (harmful) • Narcotic Effects • Respiratory Tract Irritant • Hazardous to Ozone Layer (Non-Mandatory)
Gas Cylinder • Gases Under Pressure	**Corrosion** • Skin Corrosion/ Burns • Eye Damage • Corrosive to Metals	**Exploding Bomb** • Explosives • Self-Reactives • Organic Peroxides
Flame Over Circle • Oxidizers	**Environment** (Non-Mandatory) • Aquatic Toxicity	**Skull and Crossbones** • Acute Toxicity (fatal or toxic)

MSDS (Old Standards) vs. SDS (New Standards)	
MSDS	**SDS**
1. Company Information/Chemical Name	1. Identification
2. Chemical Identity/Hazardous Ingredients	2. Hazard(s) Identification
3. Physical Characteristics	3. Composition/Info on Ingredients
4. Fire & Explosion Data	4. First Aid Measures
5. Health Hazard Data	5. Firefighting Measures
6. Reactivity Data	6. Accident Release Measures
7. Use, Handling, and Storage	7. Handling & Storage
8. Special Protection and Precautions Information	8. Exposure Controls/Personal Protection
	9. Physical & Chemical Properties
	10. Stability & Reactivity
	11. Toxicology Information
	12. Ecological Information*
	13. Disposal Considerations*
	14. Transport Information*
	15. Regulatory Information*
	16. Other Information

*Sections 12–15 are outside of OSHA's jurisdiction but must be included.

In the event a security officer discovers or is notified about a chemical spill, the officer should immediately do the following:

- Report spills, leaks, and suspicious odors to the facility management and the security officer supervisor.
- Implement the proper emergency action plan in accordance with facility requirements.
- Call 911, if necessary.
- Evacuate the area and keep the area isolated.
- Prevent other people from entering the area; it should be treated just like a crime scene.
- If possible and safe to do so, turn off ignition and heat sources.
- Stay out of the area of a spill unless it is safe to enter; report from a distance.
- Leave emergency medical response to the professionals after the spill is contained and the area is determined to be safe.
- Let trained personnel clean up spills or leaks; security is not permitted to do so.
- Write an incident report.

BOMB THREAT (DHS GUIDANCE)

Bomb threats or suspicious items should always be taken seriously. How quickly and safely security reacts to a bomb threat could save lives, including the security officer's own. Here's what to do:

Receiving a Bomb Threat:

Bomb threats are most commonly received via phone, but are also made in person, via email, written note, or other means. Every bomb threat is unique and should be handled in the context of the facility or environment in which it occurs. Facility supervisors and law enforcement will be in the best position to determine the credibility of the threat. Security personnel should follow these procedures:

- Remain calm.
- Notify authorities immediately:
  - Notify the facility supervisor, such as a manager, operator, or administrator, or follow the facility's standard operating procedure. (See below for assistance with developing a plan for the facility or location.)
  - Call 911 or the local law enforcement if no facility supervisor is available.
- Refer to the DHS Bomb Threat Checklist for guidance.
- For threats made via phone:
  - Keep the caller on the line as long as possible. Be polite and show interest to keep the person talking.
  - DO NOT HANG UP, even if the caller does.
  - If possible, signal or pass a note to other staff to listen and help notify authorities.
  - Write down as much information as possible — such as caller ID number, exact wording of threat, type of voice or behavior — that will aid investigators.
  - Record the call, if possible.
  - For threats made in person, via email, or via written note, refer to the DHS Bomb Threat Checklist and DHS-DOJ Bomb Threat Guidance for more information.
  - Be available for interviews with facility supervisors and law enforcement.
  - Follow authorities' instructions. Facility supervisors and/or law enforcement will assess the situation and provide guidance regarding facility lockdown, search, and/or evacuation.

Finding a Suspicious Item:

Together we can help keep our communities safe — if anyone sees something that is suspicious, out of place, or doesn't look right, they should say something. (Find out more about the "If You See Something, Say Something®" campaign.) A suspicious item is any item (e.g., bag, package, vehicle) that is reasonably believed to contain explosives, an improvised explosive device (IED), or other hazardous material that requires a bomb technician and/or specialized equipment to further evaluate it. Examples that could indicate a bomb include unexplainable wires or electronics, other visible bomb-like components, and unusual sounds, vapors, mists, or odors. Generally speaking, anything that is hidden, obviously suspicious, and not typical (HOT) should be deemed suspicious. In addition, potential indicators of a bomb are threats, placement, and proximity of the item to people and valuable assets.

A security guard may encounter a suspicious item unexpectedly or while conducting a search as part of a facility's or employer's Bomb Threat Response Plan. If it appears to be a suspicious item, the security officer should follow these procedures:

- Remain calm.
- Do NOT touch, tamper with, or move the package, bag, or item.
- Notify authorities immediately:
  - Notify the facility supervisor, such as a manager, operator, or administrator, or follow the facility's standard operating procedure. (See below for assistance with developing a plan for the facility or location.)
  - Call 911 or your local law enforcement if no facility supervisor is available.
  - Explain why an item appears suspicious.
- Follow instructions. Facility supervisors and/or law enforcement will assess the situation and provide guidance regarding shelter-in-place or evacuation.
- If no guidance is provided and you feel you are in immediate danger, calmly evacuate the area. Distance and protective cover are the best ways to reduce injury from a bomb.
- Be aware. There could be other threats or suspicious items.
- Every situation is unique and should be handled in the context of the facility or environment in which it occurs. Facility supervisors and law enforcement will be in the best position to determine if a real risk is posed and how to respond. Refer to the DHS-DOJ Bomb Threat Guidance for more information.

NOTE: Not all items are suspicious. An unattended item is an item (e.g., bag, package, vehicle, etc.) of unknown origin and content where there are no obvious signs of being suspicious (see above). Facility search, lockdown, or evacuation is not necessary unless the item is determined to be suspicious.

BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

**** Refer to your local bomb threat emergency response plan for evacuation criteria***

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- **911**
- **Follow your local guidelines**

For more information about this form contact the Office for Bombing Prevention at: OBP@cisa.dhs.gov

V2

BOMB THREAT CHECKLIST

DATE: **TIME:**

TIME CALLER HUNG UP: **PHONE NUMBER WHERE CALL RECEIVED:**

Ask Caller:

- Where is the bomb located? (building, floor, room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

_____

_____

_____

Information About Caller:

- Where is the caller located? (background/level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice	Background Sounds	Threat Language
☐ **Female**	☐ Animal noises	☐ Incoherent
☐ **Male**	☐ House noises	☐ Message read
☐ Accent	☐ Kitchen noises	☐ Taped message
☐ Angry	☐ Street noises	☐ Irrational
☐ Calm	☐ Booth	☐ Profane
☐ Clearing throat	☐ PA system	☐ Well-spoken
☐ Coughing	☐ Conversation	
☐ Cracking Voice	☐ Music	
☐ Crying	☐ Motor	
☐ Deep	☐ Clear	
☐ Deep breathing	☐ Static	
☐ Disguised	☐ Office machinery	
☐ Distinct	☐ Factory machinery	
☐ Excited	☐ Local	
☐ Laughter	☐ Long distance	
☐ Lisp		
☐ Loud	**Other Information:**	
☐ Nasal		
☐ Normal		
☐ Ragged		
☐ Rapid		
☐ Raspy		
☐ Slow		
☐ Slurred		
☐ Soft		
☐ Stutter		

ELEVATOR ENTRAPMENT

In the event that someone becomes trapped inside an elevator, the security officer will be notified by a command center, dispatch, property management, or direct communication from the elevator call center or occupants in the elevator. Upon receiving a call, the security officer should follow the procedures outlined below:

- Immediately respond to the floor nearest to where the elevator car is located and establish communication with people trapped inside by speaking loudly enough to be heard through the elevator doors.
- Stay in constant verbal contact with those entrapped (for support purposes), including informing them of the estimated time of arrival of the elevator maintenance personnel/ emergency assistance.
- Should the situation require emergency medical assistance, immediately contact the fire department at 911
- Complete an incident report with all pertinent information upon release of those entrapped.

NOTE: Security personnel should not attempt to extract occupants involved with an entrapment. Only elevator service personnel, along with emergency assistance personnel (i.e., fire department) are authorized to extract occupants. If the elevator is not working properly, but no one is trapped, the situation is considered a nonemergency maintenance issue. Security personnel should make sure that a sign is placed on the elevator stating that there is a problem and notify the proper facility personnel.

NATURAL DISASTER PROCEDURE

There are numerous kinds of natural disasters, and depending on what part of the country you live in, you might find yourself in the middle of a number of different types. Of course, one of the most important things a security officer must know is what types of natural disasters can occur in the area and, secondly, the emergency plan of action at the facility. Some examples of these disasters are:

- Wildfires
- Thunderstorms
- Winter conditions
- Tornados
- Floods
- Earthquakes
- Hurricanes

In case of a natural disaster, security is responsible for coordinating with property management the implementation of the site's emergency response plan. Security should be knowledgeable in:

- The protection and safeguarding of employees on premises during an emergency
- Security measures to control and minimize damage and loss
- Drills, evacuation routes, safe meeting places
- Local emergency management contact information
- The form of emergency communication system that will be used
- What normal property operations may be limited or suspended

DISASTER RECOVERY

While most people think about preparation and what to do during an emergency, few people consider what needs to be done after a disaster occurs. The fact is, once an emergency has passed, the danger is not necessarily over. First, security personnel need to survey a property for hazards and secure it right away to help prevent injuries or further property damage. This can help to expedite the rebuilding process. The following tips can help with the recovery following an emergency event.

- Make sure everyone is safe. Stay tuned to local authorities until an official "all clear" is given. If you were evacuated, return only after authorities advise it is safe to do so.
- Look for broken glass and sharp objects, and avoid downed power lines. Never touch anything in contact with power lines, including water or puddles that may be near the downed lines.
- Work with property management on coordinating companies coming to check for gas leaks or electrical system damage. Report any problems to the applicable utility companies right away.
- Work with property management in protecting the property from further damage. Be aware of needs for temporary repairs. Take steps to help protect against vandalism or additional weather damage by securing the facility/property/area and managing access by only authorized personnel. Take photos of the damage if security has a camera or cell phone for report documentation.

Nonemergency Standard Operating Procedures

This section contains material that a security company can provide to its contract employees. The name of the security company can replace "Guard Company."

CUSTOMER SERVICE INTERACTION — CUSTOMER FIRST!

It is the Guard Company's goal to be a world-class customer service organization. In most cases, you are the client's primary experience with Guard Company. Every interaction you have with every client is a "moment of truth" about the kind of service you and Guard Company provides. If those moments of truth are positive, clients will tend to be happy with the service from Guard Company. If they are negative, clients will quickly become unhappy. In a survey by the American Society of Quality, it was determined that clients become negative toward a service provider because of an attitude of indifference by just one employee of the company. Therefore, the service attitude by every employee of the Guard Company is critical.

As a security officer, you may have thousands of contacts each day with employees, tenants, visitors, and vendors of our client. At the heart of our quest to deliver "standards beyond the standard" from the status quo in the industry. Whether it is the thousands of touchpoints per day a security officer has with employees, tenants, guests, and visitors at our client properties, or a high-level meeting one of our managers has with a client contact, this program teaches our employees to ask themselves the question — *How does this make the customer feel?*

Projecting an Attitude of Service:

The moment a service interaction begins, the client makes judgments about you and your friendliness, concerns, and ability. When you are face-to-face with a client, your professionalism and eagerness to serve are conveyed by your:

- Immediate attention
- Words
- Tone of voice
- Posture
- Eye contact
- Smile
- Handshake (if appropriate)
- Appearance
- Professionalism

A service provider's willingness to extend himself or herself on a client's behalf is the hallmark of legendary service. When it's difficult to give clients what they want, going the extra mile increases the likelihood that clients will go away pleased — even if, despite your extra effort, they don't get the desired results. When you can give clients what they want, extending yourself shows that you and Guard Company are committed to providing the best service possible.

Overcoming Difficult People:

In some cases, the person you are encountering is upset or aggravated, especially if you have to deliver unwelcome news (i.e., why their car was towed, why you can't allow access without a proper badge). In these cases, it is important to de-escalate the situation by employing the following four steps of the Service Recovery Process:

Step 1: Empathy ("I understand how this can be a frustrating situation for you")
Step 2: Apologize ("I'm sorry you are having to deal with this")
Step 3: Understand (ask questions to understand their concern)
Step 4: Resolve (offer solutions within your authority)

It is very important as you de-escalate the situation that you remain calm and empathetic, even as you are carrying out the principles of your post orders.

ACCESS CONTROL

The purpose of controlling access, which includes entrance into, movement within, and departure from facilities, is to be sure that only authorized people, vehicles, and materials are allowed to enter, move about in, and leave protected areas. This is to ensure the protection of the people, property, and operations located within the facilities. Security officers, by their presence and professional performance of duties, can discourage, detect, and detain criminals through effective access control. Criminals naturally avoid areas where the chances of being caught are high.

As a security officer working at an access control point, you are the first line of defense for the security of your post. Failure to properly identify a person attempting to gain access

could result in a serious incident. It is imperative that you perform access control procedures and enforce policies in place at your facility and that you can properly identify valid forms of identification as required.

Identification Checks:
Do not just look to see that the person has an identification card or a badge, but actually look at it. Check the picture against the bearer. Is it the same person? Has the identification card been tampered with? Your post orders will specify which identification cards are acceptable. You should be familiar with the various employee identification cards issued by your property and tenant organizations.

Access Lists:
If you have to use an access list, first check an identification card for true identity, then check the name on the access list. Access lists must be current and issued by an appropriate authority. If the individual's name is not on the list, politely explain that the area/facility has controlled access and deny that person access. If the person insists on being allowed into the area/facility, politely ask the person to wait while you follow post orders for handling such situations. Your post orders will generally require you to either contact the designated agency representative who creates/maintains the access list or contact the control center (if applicable) and your supervisor.

Logs:
After making positive identification, you may be required to have individuals sign a log prior to entry and departure. Record the time of arrival and departure from the building or access control point. The log can also be used to record the issuance and return of visitor badges and can be used to determine who is inside the controlled area or facility at any given time.

Visitor Badges:
You may be required to issue badges to visitors upon determining that they are authorized to enter. In some facilities, visitors may be required to sign in or out for the badges in a log or badge register. When cards or badges are used, they are often numbered and contain the visitor's name, the area authorized, escort requirements, duration of visit, and possibly a photo and/or signature.

Card Key Systems:
These automated systems are used to allow authorized personnel (the card key holders) access through locked doors, turnstiles, or other type of gateways into protected areas. They are essentially the same as keys except that the times of entry and departure are recorded and maintained. This allows the flow of people to be monitored and makes it possible to determine who has entered or exited a controlled location. You may be assigned to entry areas to verify personal identification, prevent more than one person passing through at one time (called tailgating or piggybacking), control property, and provide assistance.

Screening:
Some locations use walk-through and hand-held metal detectors and/or X-ray machines to assist in controlling access. These devices detect the possible presence of weapons, organic and inorganic materials, and/or incendiary devices. These detectors emit a high-pitched sound

when a metal object is detected. If you work on a post with an X-ray and/or metal detector, you will receive specific training on the equipment and will have specific instructions in your post orders on the proper use and handling of the device.

Generally, you will ask a person to completely empty their pockets into a container and place any bag/briefcase/purse on the X-ray roller. Be aware that nonmetallic objects such as objects made of plastic could be used as weapons. Examine the contents of the container and then have the person walk through the magnetometer. If you use a hand-held metal detector, sweep all areas of the person's body, holding the device two inches away (there must be no physical contact with the person being inspected). If the device sounds an alarm, have the person rechecked for metal. You must resolve all questionable alarms prior to allowing the person entry into the facility. Until you are sure the person is not concealing a weapon or injurious device, deny that person access.

Challenges and Emergencies:
If a person refuses to cooperate with access control procedures and attempts to enter the facility without following them, you must try to prevent their entrance into the facility using the appropriate level of force allowed by Guard Company's Use-of-Force Policy and facility guidelines.

During emergency situations, admit law enforcement, fire, and medical personnel immediately into the facility and direct them to where the incident is occurring. If members of the press arrive at the facility, contact the control room (if applicable) and your supervisor and do not allow access without an agency representative's permission or escort.

Check your orders for local procedures on handling contract personnel who need to enter after close of business. You may have to issue passes or require personnel to present identification and be on an access roster. When an individual claims to have been called to a building by an employee, follow your post orders for processing after-hours visitors. If the post orders require you to deny access to unauthorized personnel, and the person refuses to cooperate and/or leave the premises, call the control room (if applicable), your supervisor, or the designated agency point of contact to report the situation.

Refer to the post orders for procedures on handling other visitors. These visitors may be tours or groups sponsored by occupant agencies. If escorts are required for individual visitors or groups, know the post procedures and ensure that the visitor/group escort has accepted responsibility for the visitor/group in question.

Banned Personnel/Visitors:
If a tenant employee, contractor, or visitor named on a do-not-admit list tries to access the building, the security officer should inform the person that they are not allowed on-site, and ask the person to leave. If the person leaves, the officer should contact the control room (if applicable) and supervisor to update them on the situation. If the person refuses to leave, the security officer should contact the police and explain that a person is on-site that has been banned from the facility and refuses to leave the building.

KEY CONTROL

Key control is one of the most important functions of the security officer. Lost, stolen, or misplaced keys can seriously jeopardize the security of the entire facility. These instances can also compromise the integrity of Guard Company, the integrity of the Guard Company team at your site, or the integrity of an individual security officer. With this in mind, each officer needs to realize the importance of key control and remain conscious of the responsibilities associated with maintaining custody of facility keys. The individual keys on each ring and what they open are listed on the inventory log sheet. For access throughout the building, security may be given an access badge and a set of facility keys. These keys are sometimes master keys that can access all locks. An access badge and the keys must be carried by the officer at all times and never left unattended on the security desk. The keys are attached to a chain and belt loop that is to be attached to the officer's belt. Once all keys on the ring are verified, the keys should be attached to the belt and remain with the officer until the end of the shift. Any lost or damaged keys must be reported to the site supervisor immediately.

For our customers to feel confident in our ability to protect persons, property, and assets, all security personnel need to demonstrate the ability to properly account for all keys at all times.

Key Ring Inspection:

Upon receiving a key ring, the security officer will inspect the keys, the key ring, the key chain, and the key strap to ensure that all of the above are in proper working condition. This equipment inspection must be performed in the presence of whoever issued the keys to the officer. If there are any deficiencies observed (e.g., cracked or bent key, broken belt strap), the officer receiving the keys will:

- Notify the supervisor.
- Generate an incident report, which will include detailed information regarding the receiving of the key ring and the observed deficiency.

Key Ring Custody:

Once a key ring has been inspected and its transaction documented, the officer receiving the key ring will then secure the key ring to their person by sliding the ring's belt strap around their belt and snapping the strap closed. The key ring should be attached to the belt strap before snapping the strap closed. The key chain will be stored in the officer's pants pocket.

Each officer will wear their keys per procedure until which time the keys will be transferred to another officer. This transfer will be verified by completion of the post equipment inventory log and/or entry into the daily log of the transferring and receiving security officers.

Reporting Policy:

In the event that an officer discovers a damaged key or damage sustained to the key ring and its hardware, the officer will complete an incident report. The report will include the time the damage was observed, a description of the specific damage and when the key or key ring hardware was last observed in proper condition. If the damage is observed during an exchange of the key ring between officers, both officers will be required to contribute necessary information for an incident report.

In the event that a key cabinet key (if applicable) has not been returned within a reasonable amount of time, the control center officer (if applicable) or shift supervisor will make efforts to locate the person who signed out the key. If that person cannot be located, efforts will be made to contact another person who is affiliated with the person who signed out the key. All efforts made in attempting to retrieve the key will be documented in an incident report.

In the event that a security officer's key ring is unaccounted for or if a key cabinet key has been misplaced or lost and was not signed out, the site supervisor/account manager will be notified immediately. All officers will remain on duty even if the situation occurs at shift change. Each officer will then await instructions from the site supervisor/account manager. The site supervisor/account manager will ensure that an incident report is completed and will likewise be responsible for immediate investigation of the matter.

Key Cabinet Procedures:

Maintaining proper custody and control of the keys stored in the security department key cabinet will be the responsibility of the shift supervisor/site supervisor or lead officer on duty. The officer's key control procedures are as follows:

- Upon receiving the key cabinet key ring, the officer will inspect the key cabinet key, key ring, the key chain, and the leather belt strap to ensure that all are in proper working condition. Any observed deficiencies will be brought to the attention of the shift supervisor, and an incident report regarding the deficiency will be completed.
- The security officer will then secure the key ring to their person by attaching the ring's belt strap to their belt. The key chain will be stored in the officer's pants pocket. The officer will wear the key ring until which time the key ring will be transferred to another officer. This transfer will be verified by completion of the post equipment-inventory log.
- The security officer will complete the post equipment-inventory log at the beginning of each shift. This accounting of all security post equipment will be performed in the presence of the security officer who is being relieved. In the event of any unaccounted-for post equipment, all officers from the ending shift will remain on duty and await further instructions from the account manager or site supervisor.
- An inventory of the security key cabinet is considered part of the post equipment-inventory process. In the event of missing or unaccounted-for keys, the security officer will take immediate follow-up action.
- The security key cabinet will remain locked at all times except for when transferring a key to or from the cabinet.
- The security officer will be responsible for issuing keys and returning keys to the key cabinet. These transactions will be verified by using the key transaction log. The security officer will ensure that the log is completed in its entirety and all that information recorded is accurate.

COMMUNICATIONS

All desk security personnel, while utilizing the telephones at the facility, should follow the following procedures:

> All calls should be answered promptly and with the appropriate greeting (i.e., "Good Morning,", "Good Afternoon," or "Good Evening") followed by "This is Security Officer [name]," and "How may I help you?"

The telephone is restricted to business calls only. Neither outgoing nor incoming calls are permitted. Visitors are generally not allowed to use the phone. Direct visitors to public phones adjacent to the lobby desk area (if available). All-important calls should be documented in the Desk Officers' Daily Report.

Two-Way Radios (Walkie Talkies):

In most cases each officer working at a facility will have a two-way radio. The officer must carry a radio on channel one (1) whenever away from the security desk (the actual channels used may be determined by property or facilities management). The officer at the desk will always respond as the base unit. The radios will be kept at the front desk whenever they are not in use. The officer must make a note in their log when the radio is taken from the security office and another note when the radio is returned. The radios must be charged when not in use. Radios must be accounted for and logged on the daily equipment inventory check.

- At no time is profanity to be used on the air; remember this is punishable by the FCC in the form of a fine to the offender and a possible loss of license.
- Low but audible radio volume must be maintained in deference to employees who are working in the area, except in the situation of a real need to communicate.
- Check radios are on and operating properly before leaving the front desk area. They must be fully charged and contain a fresh battery pack as appropriate.

Be sure to turn the radio off before placing it in the charger. Failure to do this will result in the radio not charging properly and possible damage to the unit.

Tips for Use:

- Verify device operation by performing a check prior to assuming post.
- Plan your message before you transmit; be brief and concise, emergencies excluded.
- Hold the device at a 45-degree angle, approximately one to three inches from the mouth and slightly to the side.
- Key the transmit button firmly, wait 2 seconds, and then begin speaking clearly and distinctly.
- Maintain a constant pace that is not too loud or too fast.
- Listen first to ensure the channel is clear before transmitting. Do not transmit when advised to stand by.

Radio Codes:

Remember that site security operations may use codes to refer to certain locations, actions taken, or to simply reduce the need to speak in full sentences. The most commonly used

codes include "10 codes" such as 10/4 or 10/20. Other commonly used codes include the use of "Code Color" such as "Code Blue" or "Code Red." These codes are used by law enforcement, security, and hospitals across the country and can vary from organization to organization, so it is important to know and understand the codes used at your site as directed in your post orders.

REPORTING PROCEDURES: DAR/INCIDENT REPORTS

Security officers will be required to record incidents and activities on a variety of report forms, as well as issue citations for violation of company rules and safety procedures. A thorough knowledge of these report forms, and the manner in which they are to be completed, is essential. These reports serve as a medium whereby the effectiveness of the individual security officer, as well as the effectiveness of the entire program, is evaluated.

Report writing can be easy. It requires that you take the time and energy to be thorough and ensure that you are accurate. Never rush to write a report when there are more facts to be learned. When completing any reports nonelectronically, the officer should use a pen with black ink. When a mistake is made on a report, the officer will need to cross out the mistake with one line through it (example). Correction fluid should never be used on any log or report. Some other common mistakes in writing reports are:

- Reports are illegible.
- Reports are on the wrong form.
- Reports are not signed.
- Reports lack details.
- Reports are not dated.
- Report are carelessly written.

Any events observed to be out of the usual daily events should be noted on the daily activity report (DAR) or an incident report. It is better to take action and write an unnecessary report than to allow a potentially dangerous situation to remain unnoticed or unreported.

The individual security officer must complete the following reports during or at the conclusion of each shift:

Daily Activity Report (DAR):

The DAR is a record kept over a specified period of time to record necessary information. The DAR can be used as a legal document of activity during that time period. The security officer will use this form to record all log entries. All entries will have a beginning and ending time and show details of what was done during that time frame. The following rules are to be followed when keeping the shift's log:

- Each officer must record "on duty" at the time they commence duty and "off duty" upon completion of their tour of duty.
- Each officer must record in the DAR that they took possession of the keys, radios, access cards, and any other equipment issued to security.
- Any unusual circumstances (fire, false alarm, property damage) that occur, and to whom the incident was reported, will be recorded. An incident report will also be needed for larger incidents.

- All nonelectronic entries must be printed in ink. No pencil entries will be accepted. There will be absolutely no erasures or changes of any kind. Corrections or deletions may be made only by drawing a single line through the portion that is incorrect, showing that the corrected information has been entered elsewhere in the log. All such corrections must bear the initials of the person making the change.
- The log will show the normal daily events and must also reflect any unusual events or circumstances that occur. The beginning and completion times of all patrols must be entered.
- An entry will be made for status change in any door or alarmed area.

In summary, the log should accurately account for the security officer's activities and location during a shift. Properly done, a log will explain, for example, why less than six hours of patrol activity was completed by a patrol officer since the log will show what occupied the officer's shift. The completed log must be placed in the "paperwork" tray or submitted electronically at the end of each shift.

Incident Reports:

Events that would be categorized as being "out of the ordinary" should be captured on an incident report. The incident report is critical; it becomes the permanent legal record of events and transactions, it keeps management aware of security-related concerns, and it ensures that facility policies and procedures are being followed. A report is a formal written presentation of facts about something that has or has not happened that will be read by others.

A report should contain only facts and never include opinions. Always carry a field notebook with you to record the facts as they occur if you don't have the capability for electronic reporting. If you include only the facts, you will be more likely to submit a report that is concise and accurate. The following seven questions must be answered in order to have a complete report:

- **Who:** Include all persons involved. Be sure to spell their names correctly and never abbreviate; others will not understand what you are writing.

- **Where:** Tell exactly where the location of the incident was and the location of everyone involved. If people moved, explain where. Always be exact.

- **What:** Tell precisely what happened, what took place, the elements of the incident, and what may have led up to it.

- **When:** Never guess when the incident occurred; give the exact time and date. If not sure, provide a time frame (e.g., Between 1900 and 2200 hours, Date).

- **Why:** This is a difficult question to answer. Give motives if they are known, but never report hearsay or rumors. Only use firsthand knowledge if it is relevant.

- **How:** Explain the facts as they are observed or told; never include your opinion.

- **Action:** Record all actions that you took, including notification of emergency personnel, facility managers, and security personnel. Record instructions given or that you gave.

Make sure your report conforms to the "Five C's" below:

- Completeness – All the facts available are present.
- Conciseness – Get to the point.
- Clearness – Be straightforward in your language so the reader is clear on what took place.
- Correctness – Put only the facts, and ensure dates, times, names, and locations are right.
- Courteousness – Don't assume the reader knows anything about the incident; don't assign blame or responsibility.

You may be unsure if you should write an incident report or just log it on the daily activity report/log. Remember, it is always better to write an incident report; something that might appear to be minor could turn into a major problem if not reported in detail.

Other Report Forms That May Be Used:

- Sign-In Register (Time Sheet)
- Equipment Inventory Log
- Pass-On Log
- Employee Sign-In Log
- Cleaner's Sign-In Log
- Contractor/Vendor Sign-In Log
- Visitor's Sign-In Log
- Lost and Found Log

SAFETY PROGRAM

We all share the responsibility for unnecessary losses, just as we do the responsibility for preventing them. All client locations have specific safety regulations to meet the individual needs of their facilities. It is your responsibility to familiarize yourself with these requirements, the use of safety equipment, and the reporting of safety hazards.

As an employee of Guard Company, you have an obligation to perform your job as safely as possible. Our goal is to have zero preventable injuries at all locations. This goal is achievable only if you take control and ownership of your assignment by making safety a part of your job.

- Slips, trips, and falls are the no. 1 cause of injury in the workplace. Use caution when walking; watch where you are going; hold on to handrails when using stairs; and don't get distracted. Pay attention to puddles of water, oil, and other hazards that could cause you to slip and fall.
- Report safety hazards immediately.
- Never lift anything heavy without assistance from others.
- Understand the physical expectations of your assignment, and plan to prevent workplace injuries.

SECURE COMMUNITY NETWORK
SCN