PRIVATE SECURITY:

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

APRIL 2022

cjp Combined Jewish Philanthropies

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?

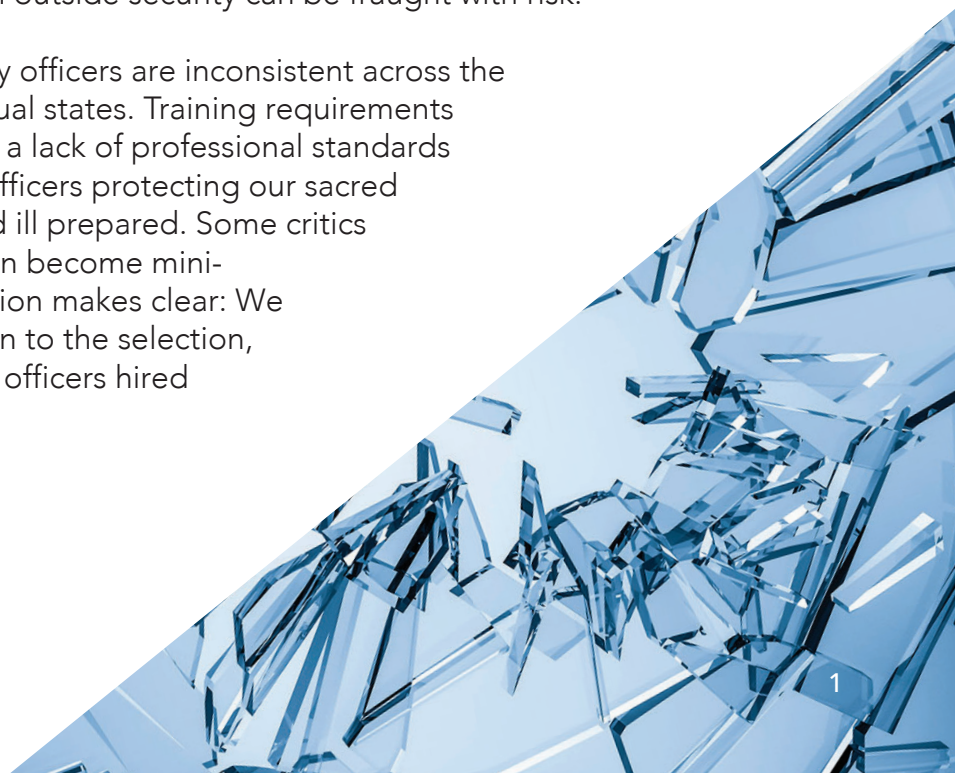
Amid the rising threat of antisemitism, as well as other acts of targeted violence and hate, Jewish communities and other faith-based organizations across North America are making significant investments in professionally managed, comprehensive security programs.

These programs bring together a number of capabilities, including intelligence and information-sharing protocols; organizational and community-wide 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?

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 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 about 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 Jewish community in North America. Although it is written from a Jewish perspective, we believe 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 regarding private security officers are woefully inconsistent at all levels. 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. 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 community-wide 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 solutions 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 can be 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.

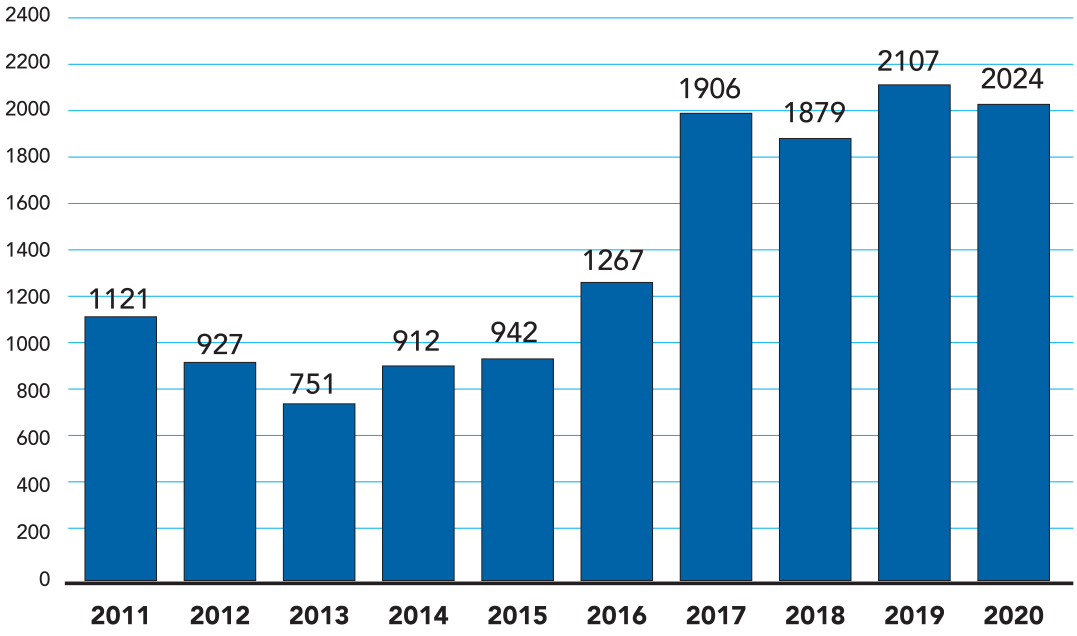
SCN serves as the Jewish community's formal liaison with federal law enforcement and coordinates closely with federal, state, and local law enforcement partners on safety and security issues related to the Jewish community; through the organization's Operations Center and Duty Desk, SCN analyzes intelligence 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 during the COVID-19 pandemic 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 identifies with racial or ethnic categories other than "non-Hispanic White" and approximately one in five Jewish adults lives 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 committees 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?

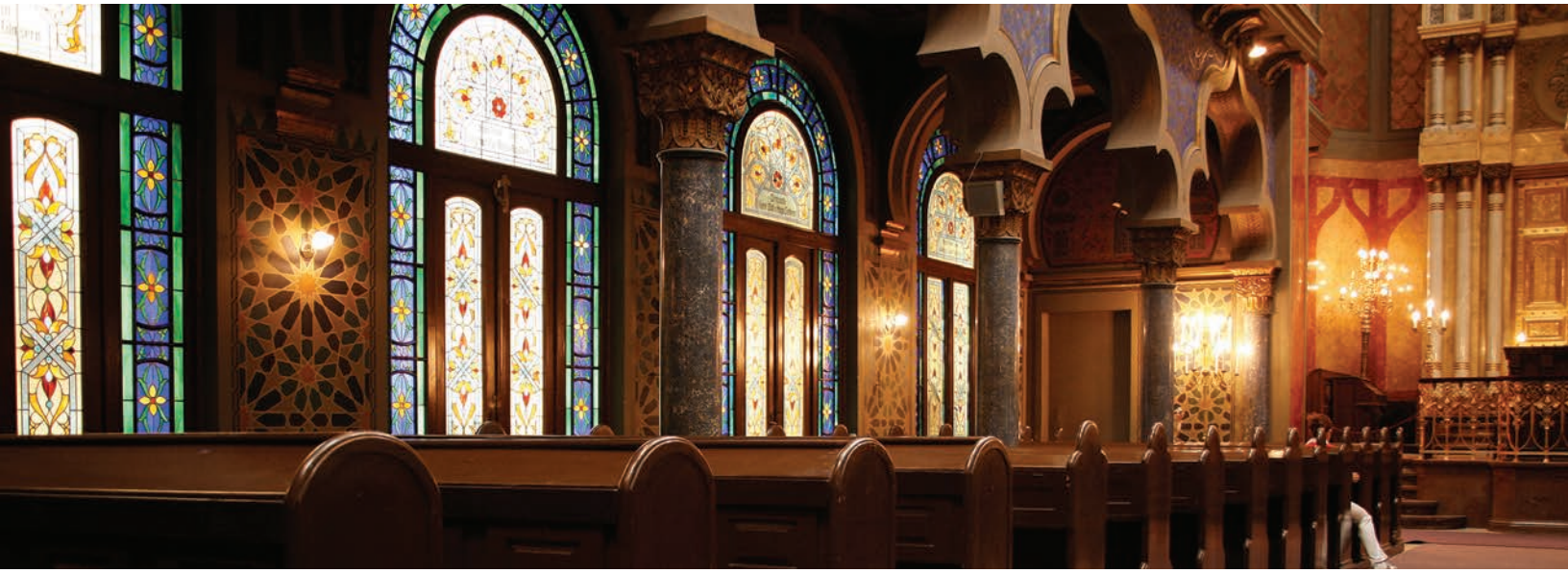
All too often, communities of faith mistakenly attempt to solve a short-term security problem with a long-term security measure, or they provide a short-term solution to a long-term security problem. For example, in the wake of events such as a mass shooting, it may be better to escalate a security presence 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?

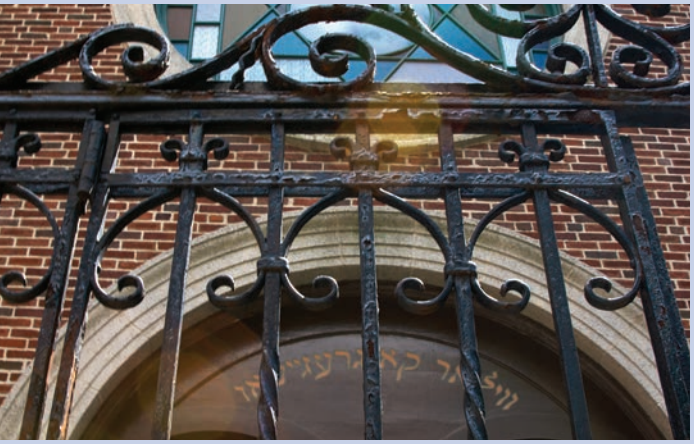
The private security company should provide information on any uniform options. Your organization should then confirm what you do or do not want your security team to wear and, if so, how the officers appear.

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. (For more information about post orders, see Pages 36 and 37.)

[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

Several 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 officer 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 officer 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. Officers' 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 officer's cost with a Jewish nonprofit, which employed that same officer during the work week. Likewise, a local Jewish day camp was able to engage a full-time security officer for its eight-week summer session since the security provider could easily redeploy that officer to work at another organization once camp ended. Third, it has led to lower turnover, greater consistency, and increased trust. Officers 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 officers become familiar faces among community members too.

What the model does not necessarily do is lead to the hiring of better officers. 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 officers, 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. Often, 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 party 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

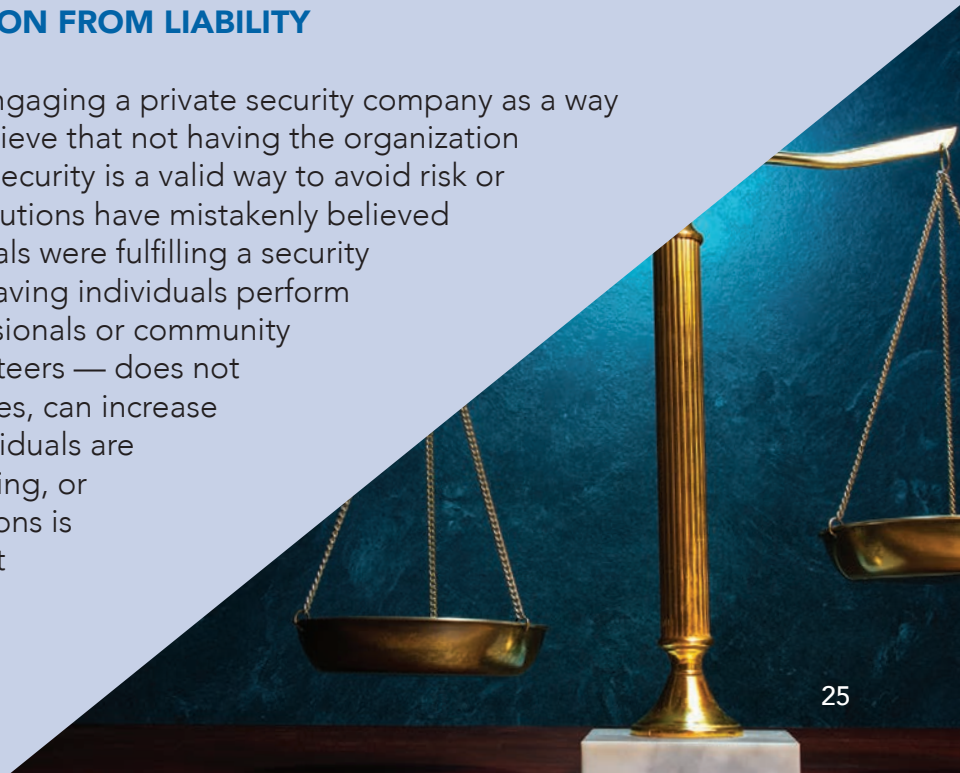
The participation of legal counsel is important to helping your organization assess potential legal risks. These can vary significantly based on the size, type, and location of your organization. Therefore, your organization's legal counsel should be tasked with identifying security laws applicable to 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 applicants 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 those 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 relative 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:

- Preemployment: 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. (For an example of some of these requirements, consult the model RFP in appendix 1.)

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 promptly removed them 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] (See Table X below. For further examples, see appendix 3.) 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 security officer service 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 provider, 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 more readily — 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 such 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 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 officers are legally allowed to conceal their firearms 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 inject 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.

CJP.Org/CommunalSecurity