BURNS McDONNELL

WHITE PAPER / **PHYSICAL SECURITY BEST PRACTICES**

BUILDING A PHYSICAL SECURITY PLAN THAT FITS YOUR NEEDS

As threats around the globe continue to highlight vulnerabilities of our rapidly changing world, cities and counties are becoming increasingly aware of the need to incorporate physical security measures into their facilities. Understanding how to begin the process is only half the battle.

In the past several years, the world has gone from learning new threat terms to realizing that simply planning for the possibility of such an event is no longer sufficient. As new threats emerge, ranging from vehicle attacks targeting random citizens to attempts to disrupt utilities in our communities, local entities are beginning to understand that preparedness and technology can provide substantial benefits.

When cities and counties are impacted by threat events, a natural reaction is to compare and identify the "right" physical security measures to protect employees, citizens and visitors. However, a lack of standardized practices for local governments makes it difficult for many entities to know where to start. Rules for federal facilities can be comprehensive and offer a starting point, but in many cases these rules are not feasible due to the significant costs associated with mitigation.

So how does one define a best practice for a specific industry? The information in this document is not intended to be comprehensive, nor to apply to all situations. Rather, it should assist the local entity in establishing a baseline that should apply to nearly any security program to provide a solid foundation that can be refined as the entity develops its physical security program.

PHYSICAL SECURITY CATEGORIES

Security comes in many shapes and sizes, and depends heavily on the level of program maturity. Whether your entity has a security project that is limited to basic security measures — from both a systematic and programmatic perspective — or you have the most sophisticated tech installed, understanding how different types of security measures complement one another can lead to creating a functional protection program.

Below is an overview of the tools nearly every city or county entity has in each security category and common things to consider in an evaluation. Finally, core minimum recommendations from our team are listed.

TECHNOLOGIES

Technology may be the first thing you think of when you think of security. As a baseline, nearly every site has door locks, alarms, fencing around potential hazards, lighting (interior or exterior) and employees.

Consider access control. As an example of technologies made to fit a specific entity, access control doesn't have to include electronic systems — it could be as simple as keeping track of who is issued what key and using a key system that can't be easily duplicated. Similarly, lighting allows people to see in a given area, but it also allows people to be seen when in that same area. Thus, considerations for new technology must take into account several variables.

Common security measures for any given entity and considerations for their implementation include:

- **Weapons screening**. Does the entity allow unknown, unscreened persons to enter restricted areas? Will the entity screen 100 percent of those who enter? What will protocols be if weapons are detected in the screening process? What equipment, staff and training are needed to operate a weapons screening program?
- **Cameras**. Does the entity plan to dedicate resources to observing camera feeds full time? Will the staff monitoring feeds be trained to detect and investigate anomalies? Does the entity want cameras to only provide forensic evidence? What equipment, network access and communications capabilities are required to properly deploy cameras?

- **Sensors.** Would responding to an alert outside of business hours help reduce possible loss or just provide earlier knowledge of a loss that has already occurred? Does the entity have infrastructure to allow notifications to be directed, based on type, to specific individuals?
- **Fencing and barriers.** Do fencing or barriers segregate areas where groups congregate from access by vehicles? Do environmental features provide opportunities for natural surveillance?
- **Electronic access control.** Does the entity require or desire access logging? Is the entity required to track entries into or exits from critical areas? What level of access to critical areas is appropriate for persons who do not work in those areas? Does the entity require on-site server or cloud-based security systems?

Core minimum: The "right" approach can vary from one situation and facility to another. A core minimum that applies to every environment and facility is to limit access to those who need it, and to create documentation (e.g. key issue log, list of authorized individuals). Without this program documentation, no program exists.

SECURITY STAFFING

Nearly all entities have a person or group of persons responsible for security related decision-making. Whether security is just an ancillary duty of the governing body or assigned to one or more specific individuals, the approach to security staffing should be based on the specific risk environment of that entity.

Smaller entities may not require more than a single person to receive and process security-related threat information, while larger entities need entire reporting structures in which similar information can cause significant changes in different departments.

Common staffing priorities for any given entity and considerations for their implementation include:

- **Getting the right people in place.** Does the entity have someone who can make decisions, based on changing information as it comes in, without oversight? Does the entity require someone to validate identities or check in visitors at entrances to buildings or critical areas? Does the entity have a mechanism for direct communication between security decision-makers and the executive leadership or governing body?

- **Training and awareness.** Can training be provided internally or does it need to be outsourced? Can training be obtained and repurposed? Are there opportunities to participate in collaborative or regional training?
- **Potential issues.** What is the desire for uniformed security staffing? What is the financial sustainability of the program?

Core minimum: When it comes to staffing, assigning an individual to the management of security-related decisions and providing this person with the authority and capacity to perform that work is essential. Building external relationships with local and regional law enforcement agencies establishes a conduit for receiving threat information. Additionally, including this person in all facility, event and organizational change meetings and discussions will provide a security perspective.

AWARENESS

Employee awareness is the most often missed security measure with the greatest potential for improvement to the overall security posture of an entity. For example, imagine a completely locked-down facility where employees who smoke step in and out of a propped-open door for their smoking breaks. Something as small as this creates enormous risk.

Features basic to nearly every entity include details as simple as knowing your co-workers and implementing open-door policies through which employees can discuss security concerns with supervisors.

Common security awareness strategies and components for any given entity include:

- Periodic staff training in security awareness.
- Periodic assessments of the physical security measures in place.
- Incorporation of threat information and intelligence.
- Escalation and de-escalation of security protocols.
- Security planning to determine the frequency of plan reviews.

Core minimum: Security should be considered important to leadership with a top-down approach of security awareness/program acceptance. Formal periodic staff training in security awareness and periodic assessments of the physical security measures in place are the minimum, as well as the inclusion of the security leadership identified above in facility, event, organizational and long-term planning discussions.

CONCLUSION

The need for physical security is only increasing. Understanding the best practices and how these rules and regulations can help state and municipal governments prepare to develop a manageable physical security plan is paramount to answering security-related questions. By utilizing a team of physical security professionals, the many pieces of the puzzle can begin to come together.

02766-PSP-0219