U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

OSAI Guidance for Use of Force Programs

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate's Office of SAFETY Act Implementation (OSAI) evaluates a wide range of anti-terrorism products, systems, and services as the subject of applications for SAFETY Act protections to be Designated or Certified as a Qualified Anti-terrorism Technology. Venue security programs and the provision of security services are two such categories of applications submitted to DHS S&T for evaluation. Providers of security services and owners or managers of venue security programs may submit applications to the DHS S&T for consideration of SAFETY Act liability protections. Venue security programs can include proprietary (employee-based) or contracted (security services provider) security officers or a combination of both.

As part of the evaluation of the safe and effective deployment of such technologies, OSAI considers an applicant's Use of Force programs which are assessed for alignment to relevant laws as well as existing consensus-based guidelines and industry standards. Such programs typically incorporate the applicant's authorization for Use of Force, inclusive of the associated policies and procedures and training. OSAI will also request and consider examples of incident and after-action reports and associated materials that may demonstrate the safe and effective Use of Force and adherence to standard operating procedures and training programs.

For more information, please click the following links:

- Use of Force Programs in SAFETY Act Applications
- General Information on Use of Force for Private Security Programs
- Documentation to Support SAFETY Act Applications by Security Services Providers and Venue
- General Considerations for SAFETY Act Evaluation of a Use of Force Program
- Use of Force Models

Use of Force Programs in SAFETY Act Applications

As stated in the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (2013), our national well-being relies upon secure and resilient critical infrastructure—those assets, systems, and networks that underpin American society. To achieve this security and resilience, critical infrastructure partners must collectively identify priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment."[1] A key area of what has become this critical infrastructure partnership is the private security industry.

Historically, most SAFETY Act applications that make use of private security forces also rely on local government police forces to provide actual criminal enforcement. More recently, U.S. police agencies have encountered staffing shortages, due to challenges in recruiting qualified candidates. In addition, as police resignations have increased, many agencies are losing officers faster than they can hire new ones.[2] Given these trends, it is also possible that critical infrastructure sites could potentially encounter lower availability or elimination of off-duty police officer employment programs in the future. These programs often provide a valuable resource to venue owners and managers as the primary or supplemental protection at a venue. Typically, in times of police staffing challenges, there are increases in the use of both armed and unarmed security officers. This suggests that the role of security officers may be changing to meet those challenges. OSAI has seen a trend of venue operators utilizing security services providers to supplement their security with additional unarmed and armed personnel.

As venue operators are increasing their use of security services providers, OSAI has noted trends in uncertainties relating to the Use of Force programs. Specifically, OSAI noted inconsistencies in the policies used by security services providers contracted to provide security at a venue versus the venue's own policies.

Security services providers are increasingly called upon to enforce venue rules and maintain order. In doing so, security personnel might be authorized by their employer, the security services provider, to respond to violent incidents, detain persons and conduct citizen's arrests pending law enforcement's arrival.[3] Similarly, venue operators' personnel may also be responsible for responding to violent

---

[1] U.S. Department of Homeland Security, "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience," (Washington, D.C., 2013), available at https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf, accessed July 20, 2023.

[2] Police Executive Research Forum, "New PERF survey shows police agencies are losing officers faster than they can hire new ones" (April 1, 2023), available at https://www.policeforum.org/staffing2023, accessed July 20, 2023.

[3] OSAI notes that applicants in the past have contended that they should not have to provide defensive tactics training or conduct background checks because their employees are not performing law enforcement duties. However, where employees are authorized to take certain actions to engage, employers should provide commensurate training to ensure the engagement is conducted in accordance with industry recognized safety procedures. See the discussion in the next section for further details and the recent California state laws that

incidents, detaining persons, and conducting citizen's arrests pending law enforcement's arrival. In such a situation, security services providers personnel and venue operators' personnel should conduct these duties using industry-recognized safety techniques and principles. Policies and procedures and training for Use of Force programs should also be based on the hazards a security officer is expected to encounter in the course of his or her duties and should be developed in accordance with existing consensus-based controls, industry standards and state and Federal government guidance. The security services provider and venue operator should submit information that demonstrates that their personnel are qualified to carry out required functions safely and effectively. When submitting an application for a Developmental Testing and Evaluation designation, a Designation, or a Certification, the security services provider or venue operator should submit information demonstrating that their personnel are qualified to carry out Use of Force functions safely and effectively.

The Department of Labor's Occupational Safety and Health Administration's General Duty Clause addresses this principle by stating that employers must protect employees from any serious hazard once they are aware of it.[4] Accordingly, for the purposes of SAFETY Act submissions, if an applicant provides or obtains security services and these services are encompassed in the application for SAFETY Act protection, OSAI asks if an applicant has taken steps to minimize or eliminate risks to the safety and health of employees from foreseeable hazards by ensuring that its security officers have the knowledge and tools to protect themselves and the public when conducting their duties.

Additionally, recent legislation in at least one state highlights changes in the regulation of the security industry regarding use of force. These changes in legislation highlight the importance of training in a Use of Force program. In October 2021, the State of California passed a law requiring specific Use of Force training for private security. AB 229 requires California's Bureau of Security and Investigative Services to develop a curriculum and mandatory training courses on the appropriate use of force for private security services employees, among other requirements.[5]

A critical component of Use of Force programs is the type of training and guidance provided to private security personnel, and this is a key component of the OSAI evaluation of security technologies. As in all SAFETY Act evaluations, OSAI considers all available current guidance on the subject of Use of Force for private security personnel in assessing the effectiveness and safety of the Use of Force programs.

---

address use of force training. Ca. Bus. and Prof. Code § 7574.18, 7583.6, 7583.7, and 7583.10 (2023), available at https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=BPC&division=3.&title=&part=&chapter=&article=&nodetreepath=5

[4] Occupational Safety and Health Act of 1970, General Duty Clause, 29 U.S.C. § 654 (2004). This clause requires employers to keep their workplaces free of serious recognized hazards.

[5] Ca. Bus. and Prof. Code § 7574.18, 7583.6, 7583.7, and 7583.10 (2023). https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=BPC&division=3.&title=&part=&chapter=&article=&nodetreepath=5

The following information is intended to assist security services providers and venue operators in preparing SAFETY Act applications.

- General Information on use of force programs for Private Security Programs
- Documentation to Support SAFETY Act Applications Submitted by Security Services Providers and Venue
- General Considerations for SAFETY Act Evaluation of use of force programs
- Use of force models

CLICK HERE TO RETURN TO UOF HOME PAGE

General Information on Use of Force for Private Security Programs and the SAFETY Act Application

Aspects of a technology security program contribute to an applicant's overall ability to provide its anti-terrorism security program under Designation Criteria 2 and 6 (Program Development and Training), Criterion 7 (Operational Effectiveness), and Certification Condition C (Safety).

In part, to demonstrate capabilities, effectiveness and safety in SAFETY Act applications involving security services, OSAI requests that applicants discuss what type of non-lethal and lethal force is authorized. Additionally, applicants should provide information about how they implement their Use of Force policies, such that their employees and contractors comply with the applicant's security directives and venue rules. Specifically, applicants should clearly indicate the standards and best practices they used to develop their Use of Force policy and the definition of force that forms the basis of their policies. In the absence of such information, OSAI uses the International Association of Chiefs of Police (IACP) consensus-based definition describing force as "*the physical effort used to control, restrain, or overcome the resistance of another.*"[6]

Security services providers and venue owners that procure contract security personnel, or that use proprietary security personnel, apply for SAFETY Act applications. Such applications should include a written use of force policy and associated training plan, regardless of whether the applicant developed and implements the policy and plan or adopts the policy and plan of its security services provider.

Prior to submitting a full SAFETY Act application, all security services providers and venue operators are encouraged to submit a pre-application to discuss the application process and Use of Force components of their technologies.

CLICK HERE TO RETURN TO UOF HOME PAGE

[6] Coalition of Eleven Organizations, "National Consensus Policy on Use of Force" (July 2020)., available at https://www.theiacp.org/sites/default/files/2020-07/National_Consensus_Policy_On_Use_Of_Force%2007102020%20v3.pdf, accessed July 20, 2023.

Documentation to Support SAFETY Act Applications Submitted by Security Services Providers and Venue

Based on years of evaluating security services applications and venue security applications, OSAI notes that some common uncertainties have existed in the area of Use of Force. Many uncertainties arise due to the lack of clear documentation of the responsibilities between a security services provider and a venue operator. Below, OSAI provides information about the types of documentation that support Use of Force components of a technology that are the subject of a SAFETY Act application. The type of information that should be submitted depends on the applicant's role of developing, updating, and implementing Use of Force policies. The guidance below accounts for these distinctions.

Security Services Providers

A security services provider (an entity providing security personnel such as security officers or event security personnel) applying for SAFETY Act protections should submit its company policies, training materials and training records relating to its Use of Force policy. A security services provider's Use of Force policies may be dependent on its customer's Use of Force policies developed by its customers. Regardless of how the policies are developed, the security services provider is responsible for providing documentation and narrative information about the Use of Force policies it has adopted and implemented. The types of documentation to support the Use of Force component will depend on who developed the Use of Force policies and training, and who is responsible for updating the policies.

The security services provider should provide the following when submitting a SAFETY Act application:

- If a security services provider provides a Use of Force policy to a customer, or develops a new policy per its customer's specifications, the security services provider should submit information about the process it used to work with that customer to develop the Use of Force program.
    - If a security services provider customizes Use of Force programs across multiple customers, the security services provider should submit internal guidance and policies for how it develops such policies for its customers and sample documentation across multiple customers supporting its approach to developing Use of Force programs.
    - If a security services provider customizes Use of Force programs, it should submit documentation about how it ensures adequate or appropriate training of its personnel to meet the requirements of the customized Use of Force programs and how such training is tracked.
    - The security services provider should submit documentation about the process for customers approving the use of the developed policy and the entity responsible for updating the policy. Examples of documentation may include a written acknowledgement from the customer that the customer understands and approves of the security services provider's Use of Force policies, procedures, and training program.

    - The security services provider should submit detailed statements of work that include any Use of Force authorization.

- If a security services provider is advised by a customer that the security services provider is expected to comply with the customer's Use of Force policies and procedures, the security services provider should submit the following:
    - Documentation that the security services provider has adopted the customer's Use of Force policies. For example, a security services provider could submit a written acknowledgement that it understands and approves the customer's Use of Force policies.
    - Documentation or a narrative demonstrating how the security services provider considers the customer's Use of Force policies as part of its risk analysis for deployment. Such documentation might include discussion of a specific deployment where the security services provider needed to develop additional capabilities, or turned down a deployment because the requested services were considered too high a risk.
    - Documentation showing how a security services provider has adapted or developed its training in line with the customer's Use of Force policies. If a security services provider relies on and adopts a policy or training materials developed by a customer, the security services provider should submit documentation identifying the source of the materials along with documentation indicating why the materials were chosen and how they have been adapted to the applicant's technology.

Venue Owners or Managers

Venue owners applying for SAFETY Act protections should provide or consider the following:

- The venue operator should submit an internal Use of Force policy, procedures and training requirements and training records.
- OSAI recognizes that a venue owner may adopt and incorporate a Use of Force policy and training program developed by a security services provider. If a venue owner chooses to submit security services provider-drafted materials, it is encouraged to submit the following:
    - Documentation that the venue owner has reviewed and adopted the security services providers developed Use of Force policy. Examples of such documentation could include a written acknowledgement showing that the venue owner understands and approves the security services providers Use of Force policies, procedures, and training for use at the venue.
    - Documentation that the Use of Force policy is updated in accordance with venue standard operating procedures for policy review and quality updates.
    - Documentation to indicate that the venue owners have worked with their security

services provider to customize the policies and training materials to address the individual needs of the venue.

  - Documentation or narrative discussion that the venue owner has reviewed the security services providers Use of Force policy it adopted to ensure the policy does not conflict with other components of the venue owner's security program, and where conflict does exist, it has been appropriately deconflicted. Such documentation should also support that the venue owner has reviewed the training requirements to ensure that the training is appropriate for the Use of Force policy and show that a security services providers training is not in conflict with the venue owner's policies.

- Venue owners who utilize or are considering utilizing a security services provider that has SAFETY Act protections should ensure the security services provider protections have not expired and do not contain restrictions or limitations related to Use of Force, to use of firearms, or any other relevant components that are in conflict with the venue owner's policies.

CLICK HERE TO RETURN TO UOF HOME PAGE

General Considerations for SAFETY Act Evaluation of a Use of Force Program

Applications for security services or venue security programs should provide the following in response to the applicable questions contained in the Application for SAFETY Act Designation and Application for SAFETY Act Certification:

- Written policies and procedures that define the authorized Use of Force and force model.
- A force model that clearly defines approved and prohibited tactics.
- Policies that are clear, concise, and free from inconsistencies.
- Policies that include a component to guide security officer decision making.
- Training reflective of the written policy.
- Practical training on the authorized tactics to enable employees and contractors to safely conduct their duties.
- A testing plan and records illustrating the implementation of training and the competence of personnel receiving training.
- Management oversight of the proper performance and adherence to Use of Force policies, procedures, and training.

The levels of force addressed in Use of Force programs include non-lethal (i.e., verbal commands, hands-on escorting, and physical restraint; and lethal force (i.e., firearms). Less-lethal force can include the use of chemicals, primarily Oleoresin Capsicum (pepper spray), conducted energy devices (Stun and Taser devices) and impact weapons (straight and collapsible batons). Security officers also apply force through use of restraint devices (handcuffs).

Documentation must clearly reflect technologies where security officers are trained and deployed to strictly observe and report incidents, but do not otherwise respond to incidents. In such cases, Use of Force is typically prohibited.

OSAI's evaluations frequently note discrepancies in the content and wording of Use of Force policies. When preparing a SAFETY Act application for security services or venue security programs, please consider the following.

Use of Force Policies

- A written detailed Use of Force policy must be provided when employees and contractors are expected to maintain order by enforcing venue rules, prohibiting access to restricted areas, reacting to field incursions and trespassing, conducting crowd control, intervening in confrontations and fights, conducting ejections and escorts and by managing aggressive or resistant persons.

- A description of the range of physical force (between lethal force and non-lethal force) that is authorized by the security services providers and venue operators must be addressed. Where

force is authorized, specific actions, tactics, and control holds that are allowed should be defined in detail.

- Security services providers and venue operators should define those specific individuals or category of employees and contractors that are authorized to use force.

- Where no Use of Force is authorized, a policy should state this, and address the circumstances under which employees and contractors are expected to disengage from public interaction and defer the maintaining of order to law enforcement. Policies often state that force is ONLY authorized for defense of self or another under threat of imminent harm. In this case, security services providers or venue operators are authorizing certain actions in certain situations, and as such their employees, should receive defensive tactics and self-defensive training to carry out those duties safely and effectively.

- Security services providers, or venue operators employing security services providers, should ensure personnel guidance is provided through a single Use of Force policy that is specific to the venue or venues. Venue operators may defer to a contractor-developed policy, however, are responsible for incorporating this into a corporate-level venue-specific policy and should provide sufficient documentation indicating the venue operator has incorporated the policies.

- Use of Force policies should include a force model, continuum, or graphic that provides a detailed description of the authorized series of actions that security personnel may take to resolve a situation. This should be based on local needs, requirements and capabilities as well as on Federal, State and local laws and guidelines. A policy should encourage but not require security officers to use de-escalation techniques in a situation before resorting to a specific level of force, unless such options can safely be implemented and are 'objectively reasonable' in light of the facts and circumstances confronting that security officer at the time. SAFETY Act evaluators will take note of variables that could affect the reasonableness of such options, including the existence of defensive tactics training, existing staffing levels, communication training, and availability of adequate levels of on-site law enforcement. Accordingly, security services providers and venue operators should address such elements in their policies and training.

- Use of Force policies should include discussions and rules surrounding use of firearms and application of deadly force.

- Use of Force policies should include a reporting and incident review component.

OSAI's evaluations have noted that Use of Force policies are often inconsistent with other materials contained in an application. OSAI has noted that Use of Force is typically presented in one of three ways: authorized for all operations, not authorized under any circumstances, or conditionally authorized.

OSAI recommends applicants provide the following information to support their Use of Force programs:

- Where no Use of Force is authorized under any circumstances, security services providers or venue operators are encouraged to ensure their policies state this unequivocally and address the potential circumstances employees and contractors might encounter where they are expected to disengage from public interaction and defer the maintaining of order to law enforcement.
- Where Use of Force is not authorized for normal operations, but is authorized conditionally, i.e., authorized for defense of self or another under threat of imminent harm, or for specific activities such as removal of trespassers on a sports field (field incursions); policies should be clear and consistent with all other application materials. Security services providers and venue operators are encouraged to ensure that the policy and other program materials reference the defensive tactics, arrest control and/ or and self-defensive training that is in place.
- Where Use of Force is authorized for normal operations, policies should address the circumstances where employees and contractors are expected to maintain order by enforcing venue rules, prohibiting access to restricted areas, reacting to field incursions and trespassing, conducting crowd control, intervening in confrontations and fights, conducting ejections and escorts and by managing aggressive or resistant persons.
- Security services providers and venue operators often designate specific individuals or categories of employees and contractors that are authorized to use force. Security services providers and venue operators should clearly identify policies defining such designations or categories and where necessary, provide narrative explanation.
- Use of Force policies should include a force model, continuum, or graphic that provides a detailed description of the authorized series of actions that security personnel may take to resolve a situation. This should be based on local needs, requirements and capabilities as well as on Federal, State and local laws and guidelines. A policy should encourage but not require security officers to use de-escalation techniques in a situation before resorting to a specific level of force, unless such options can safely be implemented and are 'objectively reasonable' in light of the facts and circumstances confronting that security officer at the time. SAFETY Act evaluators will take note of variables that could affect the reasonableness of such options, including the existence of defensive tactics training, existing staffing levels, communication training, and availability of adequate levels of on-site law enforcement. Accordingly, security services providers and venue operators should address such elements in their policies and training, and through narrative responses in the SAFETY Act application.
- Use of Force policies should include discussions and rules surrounding use of firearms and application of deadly force.
- Security services providers and venue operators are encouraged to include documentation supporting a reporting and incident review component with any Use of Force policy or in

associated program materials.

Training

- Security services providers and venue operators should ensure that all training relating to Use of Force is consistent with the overarching policy in use. Security services providers and venue operators using contract security services are encouraged to ensure that the policies, training, and curriculum the contractor developed are consistent with those of the venue.

- Training programs should define the Use of Force, excessive force, and authorized and prohibited actions by personnel. Training should occur initially, annually or on another recurring schedule, and at each different deployment, if applicable.

- In OSAI's experience, in addition to classroom training on the Use of Force and the authorized force model, practical exercises and student interaction are typically considered necessary to ensure that skill-based concepts are not simply recalled but can be practically applied.

- OSAI has found that security program training is most effective when it includes scenario-driven training, using examples that a security officer might reasonably encounter on the job, such as a trespasser running onto a playing field at a stadium (field incursion). Scenarios should emphasize the lawful and responsible Use of Force, based on the principle of using the minimum force necessary, understanding that, in situations involving an immediate threat to life, the use of minimum force may necessitate the use of lethal force. Security services providers and venue operators are encouraged to develop such training.

- Where security officers are authorized to use force, security services providers and venue operators are encouraged to include training discussing risk factors that may render a subject susceptible to serious injury or death while being restrained, such as positional asphyxia, use of prone restraints, placing body weight on subjects, etc.

- Security services providers and venue operators are encouraged to demonstrate training is provided to employees and to contract security personnel that correlates directly to the content of the Use of Force policy in operation. Training is expected to be equivalent to the types of actions that security personnel are reasonably expected to encounter depending on the venue. This typically includes education in de-escalation strategies, hands-on skills for safe control and restraint of aggressive and uncooperative persons, basic and resistive escorts, field-incursions, trespass and self-defense.

- Security services providers and venue operators should ensure that trainers have the requisite expertise and certifications to provide training.

- As part of de-escalation techniques, a force model and training should emphasize issuance of verbal warnings whenever feasible and a directive to allow the subject a reasonable opportunity to voluntarily comply prior to the application of force.

Documentation Demonstrating Adherence to Policies and Training

- Security services providers and venue operators should provide copies of incident reports involving Use of Force. OSAI will assist applicants in determining an appropriate sample size. Such reports are expected to demonstrate the effective use of a Use of Force program by showing that the actions of security officers and supervisors relating to Use of Force were consistent with the overarching policies and training in use.
- Security services providers and venue operators should also provide copies of documentation such as addendums to incident reports, after-action reports or reviews, internal investigations, law enforcement reports, or similar materials demonstrating adherence to all aspects of the Use of Force program in place. Such documentation should demonstrate that the security services provider and venue operators engage in a review of Use of Force incidents and use the results of that review to validate the Use of Force program or to make improvements. This is considered part of a security services provider's and venue operator's quality control process.
- Security services providers and venue operators should provide documentation demonstrating the overarching management of their quality control program. This includes, for example, materials illustrating that program materials are kept current with emergent threats and materials showing a comprehensive review of Use of Force incidents.
- Security services providers with large enterprises often face challenges when demonstrating or providing information about the quality control of a Use of Force program, since they often use a decentralized operating model, and because the services offered, and the Use of Force authorized can vary widely at different deployments. As part of a quality management system, security services providers should implement a centralized incident reporting system to collect all Use of Force incident reports and a procedure to conduct and report incident analysis across the enterprise. These measures could be used to validate the Use of Force program or to make improvements.

CLICK HERE TO RETURN TO UOF HOME PAGE

Use of Force Models

A Use of Force program should clearly define the authorized force options available to security officers, such as presence, verbal commands, control techniques, and self-defense techniques. It should define those techniques and actions that are prohibited, such as chokeholds and carotid restraints. These are the guidelines on the amount of force that may be used against a resisting subject in a certain situation. These are typically referred to as a force options model, or a Use of Force continuum (ladder escalation, wheel, etc.). In the past, the industry standard recommended implementing a continuum-style approach designed to explain when to use a range of force options based on the corresponding actions of an aggressive subject. More recently, law enforcement agencies, including the Department of Homeland Security, and private security industry are moving away from this continuum-style approach in favor of a force model that trains personnel to make Use of Force decisions based on the standard of reasonableness test established for the Use of Force by sworn peace officers in government employment.[7] Much of the private security industry has adopted the reasonableness test as a model, while understanding that security officers are not subject to the same restrictions as law enforcement.

No matter what type of force options model or continuum an applicant chooses to adopt, it should not require security officers to use or try lesser alternatives, such as de-escalation tactics, to work up to reasonable force. A Use of Force program should include decision-making training to guide security officers in how to determine if Use of Force is justified, and if so, when and how it should be used. Security officers who use force must be able to explain why the application of force was reasonable and necessary in the circumstances. Use of force models or continuums should consider that there may be a range of responses that are reasonable and appropriate under a particular set of circumstances. These might include, for example:

- The immediacy of the threat: can the security officer move away from the threat and wait for assistance?
- The nature of the threat: is the attacker obviously armed or exhibiting threatening behavior?
- The reasonableness of the response: is the security officer's response equal to the threat? Is it likely to cause serious bodily harm or death?
- No readily available, less harmful alternative responses: is the proposed response the least harmful option under the circumstances? Or, are less harmful responses possible? E.g., could a trespassing spectator at a sporting event with no obvious harmful intent be moved off the field with warnings, or by containment techniques, in lieu of a body slam tackle or similar aggressive move involving physical contact?

In developing policies for Use of Force models or continuums, applicants could consult the resources listed below. In reviewing these resources, and the elements of Use of Force programs discussed in this

[7] *Graham v. Connor,* 490 U.S. 386 (1989) Supreme Court case describing test used by courts to determine whether a law enforcement officer's use of force during an arrest was excessive.

document, keep in mind the following:

1. The SAFETY Act is a voluntary program designed to incentivize the development and widespread deployment of effective anti-terrorism technologies, services and capabilities. Applications are evaluated based on criteria published in the Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) at 6 Code of Federal Regulations, Part 25.
2. Hence, these resources are not a list of specific requirements, but a guide for venue owners, operators, and security professionals to use as appropriate to strengthen anti-terrorism security for venues and services. Besides strengthening venue security and security services, implementing the resources appropriate to specific technologies should assist an applicant in preparing a successful application for SAFETY Act coverage.
3. Some of the resources listed are specific to sworn law enforcement officers and not private security. However, the private security industry typically develops its foundations on law enforcement principles, as appropriate.
4. These resources should not be considered a comprehensive guide that includes all elements of a use of force program. This guide focuses policy development, training, and safety. While these aspects are critical, there are other areas for which metrics and measures of effectiveness should be developed.

Resources

- U.S. Department of Homeland Security, "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience," (Washington, D.C., 2013), available at https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf.
- *Graham v. Connor*, 490 U.S. 386 (1989). (Supreme Court case describing test used by courts to determine whether a law enforcement officer's use of force during an arrest was excessive.) Private industry has adopted the premise set forth in this case.
- Mayorkas, Alejandro N., Secretary of Homeland Security, "Update to the Department Policy on the Use of Force," Policy Statement 044-05 (Revision 01) (February 6, 2023), available at https://www.dhs.gov/sites/default/files/2023-02/23_0206_s1_use-of-force-policy-update.pdf.
- American National Standards Institute and ASIS International, "Management System For Quality Of Private Security Company Operations- Requirements With Guidance. ANSI/ASIS PSC.1-2012 (R2017)"§9.5.2 "Rules for Use of Force and Use of Force Training" An American National Standard, (March 5, 2012).
- Occupational Safety and Health Act of 1970, General Duty Clause, 29 U.S.C. § 654 (2004). This clause requires employers to keep their workplaces free of serious recognized hazards.

- United Nations Office on Drugs and Crime, “Handbook On The Use Of Force By Private Security Companies,” (Vienna, 2020), available at: https://www.unodc.org/documents/Maritime_crime/19-02086_Private_Security_Company_Handbook_Maritime_Crime_ebook.pdf.
- Coalition of Eleven Organizations, “National Consensus Policy on Use of Force” (July 2020)., available at https://www.theiacp.org/sites/default/files/2020-07/National_Consensus_Policy_On_Use_Of_Force%2007102020%20v3.pdf.
- Ca. Bus. and Prof. Code § 7574.18, 7583.6, 7583.7, and 7583.10 (2023). https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=BPC&division=3.&title=&part=&chapter=&article=&nodetreepath=5

CLICK HERE TO RETURN TO UOF HOME PAGE