

3.8. Security equipment and use of force

A. Private security personnel may not always have equipment that allows for a graduated use of force or may carry inappropriate weapons and firearms. This may result in the excessive use of force.

.....

GOOD PRACTICES*

Conduct/update risk and impact assessment (See Challenge 3.1.a.)

- ▶ Examine applicable private security laws and other national legal requirements and identify authorised weapons, firearms and ammunition for PSPs, as well as any required equipment licenses.
- ▶ Identify trends in cases of human rights abuses in which local PSPs have been involved and assess whether the lack of appropriate equipment was one of the causes.
- ▶ Assess risks versus need for armed private security. Weapons and firearms should only be authorised if their use reduces the risk of violence. "In some contexts armed protection is inescapable, as arms-carrying forms part of the 'local security culture' (...). In these contexts, the use of armed protection is so common that by not following this practice, (a company) exposes itself as a soft target." (EISF: 15)
- ▶ Evaluate the PSPs equipment, as well as the company's own equipment on site.
- ▶ Assess the extent to which PSP personnel are also affiliated with public security and/or have other ways of accessing weapons and firearms not provided by the PSP.

Match the authorised security equipment on site to the security risks and threats identified

- ▶ Develop guidelines for the use of force (e.g. use of force continuum) by PSPs and in-house security personnel which reflects the security equipment authorised by the company.
- ▶ Establish site controls to ensure safe handling and maintenance of equipment.
- ▶ Re-evaluate security equipment required on site as security risks and threats evolve.

Adopt the ICoC or develop a code of conduct for PSPs based on the VPs and/or the ICoC and make this code a standard part of all contracts issued by the company

Request that each applicant provides background information in order to assist the company in assessing their application in terms of equipment and training capabilities as part of the Request for Proposals (RFP) (See Challenge 3.2.a.)

3.8. Security equipment and use of force

“Evaluate bids in two stages; automatic exclusion on the basis of set criteria and the assessment of tenders according to award criteria” (SCG: 4) (See Challenge 3.2.a.)

1. The exclusion criteria related to equipment and the use of force should consider:
 - Failure to submit the required documentation, such as proof of equipment licenses (particularly as these relate to weapons and firearms) and training certificates.
 - Conviction of the company or its management for an offence concerning its professional conduct related to excessive use of force. (SCG: 4)
 - Proven breaches of or complicity in breaches of international humanitarian and human rights law (including through its business relations with subcontractors, subsidiary corporations and ventures).
 - Independent reports and/or proceedings before international or regional fora (e.g. OECD National Contact Points, Inter-American Commission on Human Rights) involving abuses by the PSP.
2. The award criteria related to equipment and the use of force should take into account:
 - Training on human rights, international humanitarian law (in situations of armed conflict), use of force and firearms, crowd management, conflict-diffusion techniques, and other skills.
 - PSP policies or procedures for procurement and management of weapons and ammunition based on local and international legal and regulatory requirements. These should address:
 - “Compliance with registrations, certifications, and permits;
 - Acquisition;
 - Secure storage;
 - Controls over their identification, issue, use, maintenance, return, and loss;
 - Records regarding when and to whom weapons are issued;
 - Identification and accounting of all ammunition and weapons; and
 - Proper disposal with verification”. (PSC.1: 20)
 - Proof of legal acquisition and authorisations for the possession and use of weapons and ammunition required by applicable law. (ICoC: par. 56)
 - Other equipment: communication tools and systems, IT hardware and software, uniforms, vehicles, defensive equipment.
 - Technical support: surveillance/CCTV, guard control system, access control system, alarm installation, central monitoring system.
 - “Existence of monitoring and supervisory as well as internal accountability mechanisms, such as:
 - a) Internal investigation and disciplinary arrangements in case of allegations of wrongdoing by its personnel;
 - b) Mechanisms enabling persons affected by the conduct of the personnel of the (PSP) to lodge a complaint, including both third party complaint mechanisms and whistleblower protection arrangements”; (MD Part 2: par. 12)
 - c) Regular performance reporting and specific incident reporting to the company and, if appropriate, to the relevant authorities; (MD Part 2: par. 12)
 - d) Requirement for PSP personnel and its subcontracted personnel to report any misconduct to the PSP’s management or a competent authority. (MD Part 2: par. 12)

3.8. Security equipment and use of force

Agree with the PSP on the procedures for the use of force, the authorised security equipment and the required training during contract negotiations

Develop a contract with the PSP that includes clear clauses and performance requirements on equipment and training standards, and discuss these with the PSP to make sure the security provider understands its performance objectives (See Challenge 3.2.c.). These clauses should require the PSP to:

- ▶ Provide all personnel with appropriate training with regard to the rules on the use of force, based on the standards contained in the VPs, the ICoC, the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, and “national laws or regulations in effect in the area duties will be performed”. (ICoC: 13)
- ▶ Provide all necessary security equipment to their personnel (e.g. protective equipment, non-lethal arms and, if required, lethal arms), including safe carry and concealment systems if they are to carry firearms.
- ▶ Ensure that private security “personnel who are to carry weapons will be granted authorisation to do so only on completion or verification of appropriate training with regard to the type and model of weapon they will carry. Personnel will not operate with a weapon until they have successfully completed weapon-specific training” and they “must receive regular, verifiable and recurrent training specific to the weapons they carry and rules for the use of force”. (ICoC: par. 58)
- ▶ Control the day to day use and deployment of weapons, firearms and ammunition.
- ▶ Guarantee that under no circumstances will its personnel carry and use weapons or ammunition which are illegal under any applicable law, nor will they alter weapons and ammunition in any way that contravenes applicable national or international law. (ICoC: par. 57).
- ▶ Ensure that off-duty public security officers working for the PSP do not bring their weapons, firearms or ammunition to the company premises.
- ▶ Report any incident involving its personnel that involves the use of any weapon and conduct an internal inquiry in order to determine the following:
 - a) “Time and location of the incident;
 - b) Identity and nationality of any persons involved including their addresses and other contact details;
 - c) Injuries/damage sustained;
 - d) Circumstances leading up to the incident; and
 - e) Any measures taken by the (PSP) in response to it.

Upon completion of the inquiry, the (PSP) will produce in writing an incident report including the above information, copies of which will be provided to the client and, to the extent required by law, to the Competent Authorities”. (ICoC: par. 63)

If the PSP is unable to provide the necessary equipment to its personnel, consider whether the company should provide any of this equipment to the PSP (See Challenge 3.8.b.)

3.8. Security equipment and use of force

If the PSP fails to comply with any or several of the clauses in the contract, consider the following options:

- ▶ Negotiate a timeline for compliance.
- ▶ Withhold payments as established in the contract until the issue is satisfactorily addressed.
- ▶ Condition ongoing relationship on performance and provide further, detailed guidance and training, together with regular performance review.
- ▶ Terminate the relationship with the PSP.

In cases of breaches of national and/or international law by PSPs, report the incident to the relevant authorities and stakeholders and take the necessary steps to address remedy and prevent future similar incidents ([See Challenge 3.10.a.](#))

3.8. Security equipment and use of force

B. Companies may find themselves with little other option than to provide the PSP with the necessary equipment to effectively perform their functions.

GOOD PRACTICES*

Take all appropriate measures to ensure the PSP provides the necessary equipment to its personnel (See Challenge 3.8.a.)

If the company decides to provide equipment to the PSP, develop relevant policies and procedures and add these to the contract

- ▶ Develop a company policy for the provision of equipment to PSPs.
 - Specify the types of equipment the company may provide and its intended use.
 - Prohibit the provision of weapons, firearms or ammunition to PSPs.
 - Prohibit the transfer, loan or sale of equipment provided by the company to a third party. (BP: 13)
 - Establish clear procedures for the handing over of any equipment, ensuring it is all kept on record.
 - Require written commitment by the PSP to respect human rights and international humanitarian law.
 - Require the storage of equipment in the company's facilities.
- ▶ Establish monitoring procedures to supervise the use of equipment.
- ▶ Refer to the incident reporting mechanism included in the contract (or develop one if none is in place).
- ▶ Add the company's policy for the provision of equipment to PSPs and the related monitoring and incident reporting procedures to the contract with the PSP. Termination conditions should be included in the event that security equipment is misused. (BP: 13)

Agree on a training programme with the PSP for guards assigned to the company's operations (See Challenge 3.6.a.) with a special focus on the rules for the use of force

- ▶ Refer participants to the UN Code of Conduct for Law Enforcement Officials, the UN Basic Principles on the Use of Force and Firearms, the International Code of Conduct for Private Security Service Providers and "national laws or regulations in effect in the area duties will be performed." (ICoC: par. 59).
- ▶ Address the following topics:
 - Reasonable steps to avoid the use of force;
 - Use of force continuum including force de-escalation techniques to resolve threats with minimum necessary force;
 - Compliance with all national and international obligations;
 - Proportionality to the threat and appropriateness to the situation; and

3.8. Security equipment and use of force

- “Self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life”. (PSC.1: 24)

Supervise the performance of PSPs and the use of equipment provided by the company through regular monitoring

- ▶ Monitor PSPs through a variety of means: radio networks, CCTV visual monitoring (including installing cameras in security response vehicles), unannounced physical site inspections and regular personal equipment inspections.
- ▶ Support the oversight of PSPs by local authorities and community groups. (OECD: 215)
 - Develop a network with relevant stakeholders, ensuring the different groups in local communities are adequately represented (in particular the most vulnerable groups), and provide them with some guidance on what to do whenever there is a risk of a human rights abuse.
- ▶ Check all complaints against the PSP reported through grievance or any other mechanisms and record all allegations of human rights abuses by private security. ([See Challenge 3.10.a.](#))

Engage with relevant stakeholders to develop performance monitoring mechanisms for PSPs

- ▶ Identify and engage with stakeholders with close knowledge of PSP activities and impacts (e.g. home governments, other companies, civil society organisations).
- ▶ Explore how existing mechanisms (e.g. ICOCA, local mechanisms) can support monitoring.
- ▶ Exchange information about unlawful activity and abuses committed by PSPs. (VPs: 7)

Conduct investigation into credible allegations and any incident involving the inappropriate use of equipment or force and, where appropriate, report abuses to the relevant authorities ([See Challenge 3.10.a.](#))

- ▶ Establish whistleblower protection mechanisms that guarantee protection of sources.
- ▶ Integrate any lessons learned into future training provided to PSPs.