

### 3.7. Relationship between public and private security

**A. In some countries public security personnel work for PSPs when off-duty. This may create confusion over roles and responsibilities, which may lead to inappropriate practices, in particular with regard to the use of force, apprehension and detention.**

.....

#### GOOD PRACTICES\*

As part of the risk and impact assessment, consider risks and potential impacts of using public security personnel as private security providers

- ▶ Assess the capabilities, practices and human rights track record of public security forces.
- ▶ Analyse the legal framework that regulates the private security industry and find out if it is legally allowed for public security personnel to work for a PSP when off-duty. If legal, ensure the assessment provides a clear picture of any restrictions and conditions.
- ▶ Consider focused stakeholder engagement with affected communities to identify any additional concerns and/or risks associated with the use of public security as private providers.

Request a letter of consent from the relevant public security institution stating that the concerned individuals are allowed to work for a PSP

Conduct a training needs analysis during contract negotiations with the PSP and agree on a training programme with the provider based on the results, including who will deliver what part of the training (i.e. the company, the PSP or a third party).

- ▶ Ensure the training programme follows the recommendations listed in [Challenge 3.6.a.](#), with a special focus on the following elements:
  - Differences in the mandate and responsibilities between public and private security roles.
  - Rules for the use of force and firearms. 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) It is essential that public security officers working as private security understand the different rules applicable to the provision of private security services, to law enforcement operations and to the conduct of hostilities in situations of armed conflict (i.e. when international humanitarian law applies).
  - Use of force training that addresses:
    - 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;

## 3.7. Relationship between public and private security

- “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” (PSC1: 24); and
- Weapon-specific training for all personnel who are to carry a weapon.
- Restraining or apprehending individuals.
- Practical exercises that include locally-relevant scenarios and possible contingencies to put all of the above into practice. Start by providing a background briefing to PSPs on local conditions, operating environment, risk assessment findings and stakeholder engagement observations. Communicate all tasks and expectations to participants; discuss each step of the actions and responsibilities of participants; and run-through the whole scenario with role-players. (MIGA: III-9) When feasible and relevant, public security should also participate in these exercises, this will help participants understand their different roles and responsibilities in the event of an incident.
- Include the details and conditions regarding the training programme in the contract.

**Complement the training with additional measures**

- Request supervisors to deliver short talks focused on key principles of the VPs and the code of conduct for PSPs regularly.
- Provide supporting materials (e.g. pocket book with key aspects of the code of conduct for PSPs).
- Identify and engage with ‘champions’ within the public security sector that due to rank or status can effectively promote good practices with colleagues.

**Ensure that all private security personnel working on the company’s site wear the PSP or company uniform**, which should be clearly distinguishable from the public security uniform, and are “individually identifiable whenever they are carrying out activities in discharge of their contractual responsibilities” (ICoC: par. 43). Having a distinct uniform for each job may help personnel differentiate between their two roles.

**Ensure that off-duty officers do not bring their weapons, firearms or ammunition to the company premises**

## 3.7. Relationship between public and private security

**B. Companies working with both public and private security may face multiple lines of command, poor communication, inadequate coordination, and resulting difficulties in investigating human rights abuses.**

.....

## GOOD PRACTICES\*

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

- ▶ Analyse the structure, functioning and performance of public security forces.
- ▶ Identify specific challenges in the interaction between public and private security.

**Meet with the chain of command of public security forces and other government stakeholders at the regional and/or local level** (See Section 2.1. “Security arrangements”), before finalising private security arrangements

- ▶ “Clearly communicate private security plans and arrangements to assigned public security and other government stakeholders” (IGTs: 54), sharing information from the risk assessment.
- ▶ Raise the VPs and international standards on the conduct of both public and private security providers.
- ▶ Seek agreement on the different roles assigned to public and private security. On this basis, agree with the chain of command of public security forces the rules for their deployment around the company’s facilities, in particular try to determine mechanisms and procedures for scaling up or down depending on the changing environment.
- ▶ Only request the permanent deployment of public security forces if there is a high level of lawlessness, or if “the site is so remote that the response time for public security forces to arrive exceeds the ability of the company’s private security (providers) to manage security risks and protect the site”. (MIGA: III-8)
- ▶ Request the management of public security to designate points of contact at each relevant level in the chain of command.
- ▶ Establish formal and consistent reporting and communications mechanisms between public security forces, the company and its PSPs.
- ▶ Agree on a process for investigations of human rights abuses.
- ▶ Establish a written agreement or MoU with the local management of public security reflecting all of the above, or consider substitute measures in the absence of a MoU (See Section 2.3. MoUs).

**Finalise negotiations with the selected PSP and establish a contract including specific requirements regarding the PSP’s engagement with public security** (See Challenge 3.2.c.)

- ▶ Define clearly the different roles and responsibilities of public and private security.
- ▶ Share information on public security arrangements around the company’s site, as well as on any agreements reached with the public security forces chain of command.

## 3.7. Relationship between public and private security

- ▶ Require the PSP to designate a focal point for liaising with the company's security department and with public security points of contact.
- ▶ Establish reporting and communications mechanisms based on the agreement with public security.
- ▶ Clarify what equipment is available and who can use it.

Following prior agreement with the public security forces chain of command, encourage the organisation of joint drills involving public security working in the company's area of operations, the PSP and the company's in-house security

- ▶ Clarify roles, responsibilities and reporting lines, and promote information sharing between different actors.
- ▶ Ensure joint drills "address the phases of an incident response including:
  - Preparation and review of rules (for the use of force),
  - Alert,
  - Deployment,
  - Designation of the on-site team leader,
  - Actions on contact,
  - Resolution of the incident,
  - Provision of medical attention (and evacuation) if required,
  - Review of post-incident lessons learned,
  - Final reporting and follow-up." (MIGA: III-9)
- ▶ Consider inviting relevant local stakeholders to these exercises. This will promote understanding of the different roles and responsibilities of public and private security.

Set regular meetings to discuss security arrangements (e.g. once a month) with the appointed points of contact for both public security forces and the PSP, as well as ad hoc meetings immediately after an incident. These meetings should address any relevant security related updates in the area.

Coordinate with other companies operating in the area

- ▶ Share experiences on working with both public and private security; identify key challenges and lessons learned.
- ▶ Seek coherence in security practices, in order to prevent confusion on the roles of different security actors.
- ▶ Consider developing a contingency plan in case public security previously assigned to the company's area of operations become unavailable.

## 3.7. Relationship between public and private security

**C. Where public security response times are inadequate, or where company operations are located in remote areas, it may be necessary for PSPs to act as first responders in high risk situations, or to otherwise deal with situations that are normally the responsibility of public security forces.**

.....

## GOOD PRACTICES\*

### Conduct needs assessment

- ▶ Assess company needs against the capacity of public security forces. The needs assessment should focus on issues such as training, equipment, transportation and communications.
- ▶ Measure average response times for public security forces to get to the project site in an emergency.
- ▶ Identify additional training and equipment needs of private security personnel.
- ▶ Assess alternative available solutions, including community led or third party (international organisation, home government associated) assistance.

### Update risk assessment

- ▶ Analyse relevant past security incidents where public security response was required and identify trends, if any.
- ▶ Assess whether providing logistical, financial or in-kind support to local public security (e.g. providing training or communications equipment) can improve public security's ability to respond. Consider whether other actors (e.g. home governments, human rights institutions, international organisations, multi-stakeholder initiatives) can address gaps through capacity building, training and other assistance activities. If this is not feasible, balance benefits against possible negative consequences of providing such support. (See Section 2.6. Equipment)

### Engage with a wide variety of stakeholders

- ▶ Engage with host government actors and the command of public security forces at the national, regional and local levels to identify appropriate means of addressing this challenge.
- ▶ Meet with other companies operating in the area, if any, to share experiences and concerns and to pool efforts in improving the situation.
- ▶ Consult with international NGOs, civil society organisations and local communities to discuss risks and impacts associated with the current situation and to jointly identify possible solutions.

### Establish early warning mechanisms that allow the company to request public security support with sufficient time for them to arrive before situations become violent

- ▶ Develop an information sharing system with other companies and local stakeholders (IGTs: 42). This can help identify local tensions before they develop into high risk situations.

## 3.7. Relationship between public and private security

- ▶ Consider establishing a multi-stakeholder security forum to discuss security and human rights issues. The forum should include representatives from local communities, ensuring the most vulnerable groups are adequately represented.
- ▶ Identify early warning signs based on research on past security incidents conducted as part of the risk assessment.

**Consider providing assistance to improve the response time of public security, taking into account the findings of the needs and risk assessments**

- ▶ Seek ways to improve communication and coordination between public and private security (See Challenge 3.7.b.)
  - Establish formal and consistent reporting and communication mechanisms with public security forces, including the designation of points of contact at each relevant level.
- ▶ Consider the possibility of providing logistical, financial or in-kind support to improve the response time of public security forces. (See Challenge 2.6.b.)

**Establish a security response team that can act as first responders as necessary**

- ▶ Develop response guidelines and procedures (including rules for use of force, weapons and firearms, as well as procedures for restraining and apprehending persons) and ensure response team members are trained accordingly.
- ▶ Ensure the response team coordinates with public security and retreats as soon as public security is deployed on site.

**Include a clause outlining the approach to the issue of apprehending persons in the company's code of conduct for PSPs and in the contract with the PSP**

- ▶ Stipulate that PSPs may "not take or hold any persons except when apprehending persons to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity." (ICoC: par. 34)
- ▶ Stipulate that all apprehended persons should be treated "humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment." (ICoC: par. 33)
- ▶ Stipulate that there should be no firearms in the room where the person(s) is/are temporarily detained and that force shall not be used to try to prevent people from escaping.
- ▶ Require the presence of a female guard if there are women among the apprehended persons.
- ▶ Make this provision part of the information communicated to local communities and public security authorities.

**Adjust the training programme for private security personnel on a regular basis to address findings from the needs and risk assessments (See Challenge 3.6.a.)**

- ▶ Ensure training covers all relevant aspects regarding appropriate and proportionate use of force. Use of force training shall address:

## 3.7. Relationship between public and private security

- 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;
  - “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); and
  - Weapons and firearms specific training for all personnel who may carry a weapon.
- ▶ Include a session on conflict management, crowd control, public order and apprehending persons, based on the company’s code of conduct for PSPs.
  - ▶ Explain the differences between the roles of public security forces and PSPs. ([See Challenge 3.7.a.](#))
  - ▶ Conduct practical exercises using real-life scenarios so that private security personnel learn good practices in responding to high risk-situations in an effective way, and in compliance with the standards expressed in the VPs, the ICoC and the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

If the above recommendations are not sufficient to properly manage security risks, consider requesting the permanent deployment of public security forces closer to the project site

- ▶ Engage with all relevant stakeholders (e.g. host government authorities, public security representatives, other companies, local communities) to ensure their different needs and concerns are taken into account in the deployment of public security forces.
- ▶ If the host government lacks the necessary resources, consider providing financial or in-kind support for the permanent deployment of public security forces. If the company takes this course of action, address potential risks through the risk assessment and communicate to local stakeholders.