II. Working with Public Security Forces

II. Working With Public Security Forces

2.1. Security arrangements

A. Companies may be "obliged" to work with public security, including inside their sites, without knowing in advance the numbers and operational capabilities, as well as the rules and restrictions governing public security forces assigned to their area of operations.

GOOD PRACTICES*

Discuss security arrangements with the management of public security forces at the national, regional and/or local level

- Raise the VPs and international standards on the conduct of public security forces. Emphasise that the type and number of public security forces deployed should be proportional to the threat. (VPs: 4) If national authorities decide, in compliance with national law, to deploy military forces to areas of extractive operations, highlight the need for adequate training and equipment.
- Identify and set out in formal terms 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 is too long. (MIGA: III-8)
- Consider requesting that a certain percentage of public security forces deployed are women. "Women may be able to provide different levels of attention to specific vulnerable groups and may also help avoid gender-based violence by their presence."[1]
- Assess whether the security benefit of working with public security forces (e.g. for convoy protection) outweighs the risk that lethal force may be used.

Maintain close contact with representatives of public security forces at different levels

- Seek home government support to access high-level public security officials.
- "Liaise with the appropriate ministry to corroborate ground-level information from security providers". (IGTs: 14)
- Maintain close contact with the police and military forces representatives at each echelon. (MIGA: III-14)
- Raise concerns to authorities at the appropriate level whenever use of force by public security is excessive. (IGTs: 44)

- Establish formal and consistent reporting and communications mechanisms with public security forces and other stakeholders to ascertain ongoing threat levels. (IGTs: 14, 44)
- Always document decision points in meetings with public security forces and distribute them among participants.
- Ensure the company approach to security arrangements (roles and responsibilities, chain of command, use of force, etc.) is mainstreamed through all security personnel on site.
- Sponsor visits by senior public security officials to the company's operational site. "These steps strengthen the company management's access in difficult times." (MIGA III-12)

Establish an agreement or MoU (See Section 2.3. MoUs)

- Develop a joint risk assessment process including representatives of public security forces to agree on security risks and the nature and level of support required from public security forces.
- Use any in-kind support the company provides as an incentive to agree on and enforce clear rules on deployment and conduct of public security forces that comply with the VPs, the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. (MIGA: III-7)
- "Encourage host governments to permit making security arrangements transparent and accessible to the public, subject to any overriding safety and security concerns." (VPs: 4)

Support efforts to provide human rights and international humanitarian law training for public security forces (See Section 2.5. Training)

GO BACK TO LIST OF CHALLENGES

B. In situations of armed violence, the public security forces assigned to areas of corporate operations may be considered as a military objective by one of the parties.

GOOD PRACTICES*

Analyse the context as part of enhanced due diligence and assess risks and impacts regularly

- Conduct a conflict analysis to understand the root causes, the dynamics, the actors and nature of local conflicts. The conflict analysis should also assess the level of adherence to human rights and international humanitarian law standards by the different parties. (VPs: 5)

The **conflict analysis** should offer answers to the following key questions:

- What are the root causes of tensions and potential triggers?
- Who are the main actors in the conflict? What are their motives, capacities, and opportunities to inflict violence?
- "Is conflict likely to re-emerge and/or are certain geographical areas not controlled by the state?" (OECD: 53)
- "What are the roles played by the security sector in the conflict?" (ITGNs: 70)
- "Has the security sector contributed to, or been among the root causes of, the conflict?" (ITGNs: 70)
- Which are the most prevalent conflict dynamics among regional stakeholders? (ITGNs: 72)

- Conduct a human rights/international humanitarian law assessment to identify and map sources of potential conflict. Where feasible, mandate a reputable and experienced local actor to conduct this study. (MIGA: II-16)

A **human rights/international humanitarian law assessment** should offer answers to the following questions:

- What are the main human rights and international humanitarian law violations people have faced/are facing?
- Who are the main perpetrators of the violations?
- Which are the most vulnerable groups?
- What are the scope and dynamics of sexual and gender-based violence?
- "Does a state mechanism exist to monitor, report and respond to violations perpetrated by members of the security sector?" (ITGNs: 71)
- "Are effective steps being taken to hold perpetrators in the security sector accountable?" (ITGNs: 71)
- "What measures have been taken with a view to preventing the recurrence of such violations?" (ITGNs: 71)
- "What capacity does the security sector have to prevent and respond to reports of violations by its own actors or by other actors?" (ITGNs: 71)

- ▶ Identify security risks for the company (e.g. risks for company personnel and families, facilities and assets), as well as risks for local communities. This "allows a company to take measures to minimise risk and to assess whether company actions may heighten risk." (VPs: 2)

A comprehensive **security and threats analysis**, potentially including a survey drawing on local public perceptions, should offer answers to the following key questions:

- What are the main threats to be addressed?
- "What is known about the nature of those threats: who does what, how, when, where, and to whom?" (ITGNs: 71)
- "Are there tensions between different social groups? What are the triggers that could inflame tensions?" (OECD: 53)
- Who are the "champions" at community level that could help to mitigate security risks?
- "How can the security sector contribute to mitigating these threats?" (ITGNs: 71)
- Is the security situation improving or worsening in the country?

- ▶ Conduct an impact assessment to understand the company's impact on the local context and identify ways of mitigating potential and actual negative impacts.
- ▶ Engage in community consultations regarding security measures. "Regular discussions with community members can be a good source of security risk information." (IGTs: 20) Ensure all vulnerable groups are adequately represented in these consultations

Minimise the presence of public security forces at company sites (MIGA: III-1)

- In conflict environments, try to avoid public security forces becoming involved in operations at company sites if private security can legally and practically respond to needs. Although the government also remains responsible for the conduct of public security forces, "once the company invites or requests a public security force detachment onto its facilities, the company inherently accepts responsibility for its conduct at the site." (MIGA III-8)
- Request public forces only when there is an urgent need at a specific location and then clearly define their mandate as well as the time limits for their expected withdrawal. (MIGA: III-1)

Promote respect of international standards and good practices by public security forces deployed on site

- In discussions with representatives of public security forces, underline that forces deployed should be competent and the type, number and means engaged should be appropriate and proportional to the threat. (VPs: 4) Ensure that this requirement is made explicit in an MoU/ agreement with the host state. (See Section 2.3. MoUs)
- If national authorities decide, in compliance with national law, to deploy military forces to areas of extractive operations, highlight the need for adequate training and equipment, and ensure that their chain of command is clearly defined in relation to company management.
- Designate public security forces assigned to companies' facilities as "the Security Emergency Reserve, held in readiness as a response force and not routinely used for guard duties." (MIGA: III-8)
- Ensure roles and responsibilities of public and private security are clearly defined and communicated to both public security forces chain of command and company management.

Monitor closely the public security forces assigned to the protection of the company's staff, assets and operations.

Ensure they do not take part in operations related to conflict/armed violence.

Publish policy on human rights

- Companies should openly communicate the circumstances in which public security forces are likely to be associated with their operations, as well as how they address the risk of human rights violations by public security forces in these situations. This could help to make the public differentiate between the company and the security forces that are guarding them and may reduce the risk of being too closely associated with public security operations.

GO BACK TO LIST OF CHALLENGES

C. Public security forces may suffer from insufficient human resources, low salaries, inadequate training and poor equipment. This may increase the risk that they engage in criminal activity or human rights violations.

GOOD PRACTICES*

Conduct/regularly update risk assessment

- Estimate public security resource needs as part of the risk assessment.
- Assess potential conflict risks as a result of imbalances within public security forces due to additional resources provided to units dedicated to company security.

Consider alternatives to the provision of financial and material support

(See Challenge 2.6.a.)

Engage with the appropriate government agencies and emphasise the need for the host government to provide adequate resources

- Include a provision in the agreement/MoU with the host government that part of the taxes paid by companies be used to provide resources to public security forces. (MIGA: II-17)

Support efforts by governments, civil society and multilateral organisations to strengthen state institutions (VPs: 5)

- Identify synergies with security sector reform programmes. Programmes to strengthen the management and oversight roles of security institutions as well as training for public security forces are in place in many countries. The company could engage with these programmes to extend some police reform activities to the area of the company's operations. (MIGA: II-18)
- Support programmes that promote "fair, objective, transparent, non-discriminatory and merit-based policies and practices on recruitment, salaries, performance evaluation, promotion and professional development" of public security forces. (ITGNs: 105)
- Provide resources to support programmes that strengthen accountability at the local level.

2.1. Security arrangements

SSR Programmes

There are a number of entry points that can assist companies in the identification of regional and national security sector reform programmes.

1. The **International Security Sector Advisory Team** (ISSAT) offers detailed country and region specific information on SSR programmes, resources, experts and news. The country profiles are part of the ISSAT Security and Justice Reform Community of Practice (CoP), an online platform that allows practitioners to access and contribute to a vast repository of policy guidance documents, case studies and e-learning courses. It provides a great opportunity to identify and engage with security sector reform practitioners and programmes. The country profiles can be accessed here: http://issat.dcaf.ch/Learn/Resource-Library/Country-Profiles
2. The **African Security Sector Network** (ASSN) is an extensive network of organisations from across Africa focusing on the security sector. The network includes Regional Hubs in Accra, Juba, Mzuzu and Nairobi, and promotes the cooperation and exchange of actors and organisations working in security related domains. The ASSN can be accessed here: http://www.africansecuritynetwork.org/site/index.php?option=com_content&view=article&id=142&Itemid=73
3. The **Security Sector Reform Resource Centre** provides SSR Country Snapshots, which provide up-to-date information on SSR programmes, stakeholders and donors around the world. Not all countries are yet covered by the Country Snapshots but they are continuously being added / expanded. The Country Snapshots can be accessed here: http://www.ssrresourcecentre.org/countries/
4. The **UN Security Sector Reform Website** provides an overview of international organisations, training providers and UN agencies involved in SSR programmes around the world. The website can be accessed here: http://unssr.unlb.org/.

Engage with other concerned companies to get home governments or multilateral institutions to provide the material and support needed. The company could “contribute to a consolidated programme of equipment and training that will jointly benefit all companies in the area.” (MIGA: II-18)

If the company feels compelled to provide financial and material support to public security forces, assess all potential risks and establish safeguards (See Challenge 2.6.b.)

- Assess the security benefit of providing resources to public security forces against the risks of human rights violations. If the benefits outweigh the costs and risks, establish and disseminate clear criteria for providing material support.
- Analyse any past cases of material support as the basis for the provision of such material.

Develop clear procedures for the provision of financial and material support to public security forces assigned to the project site

- Develop a protocol for the provision of equipment, goods and services to public security forces. (MIGA: II-17)

- Condition equipment transfers on the government's commitment to respect human rights and the appropriate standards and codes for the protection of individuals and the use of force in the context of law enforcement operations (human rights) and in the conduct of hostilities (i.e. where international humanitarian law applies).
- "List anything provided to governments, including public forces, in a Record of Transfer Register. The register identifies exactly what the company provided, when and for what purpose. The recipient's representative should sign a receipt for all items provided." (MIGA: II-19)
- Ensure full transparency of payments made and/or equipment transferred.

Ensure that financial and material support provided to public security reaches personnel on the ground

- Endeavour to split the payments intended to contribute to public security forces between the relevant authorities at national and local levels.
- Where public security forces are entitled to payments in the form of a per diem or supplement to enable travel to company sites, ensure these are delivered directly to individuals.
- Ensure that any equipment to be used for the protection of the project site is secured at the site and released only according to agreed procedures. (MIGA: II-19)

GO BACK TO LIST OF CHALLENGES

D. If payments (cash and in-kind) to public security forces in exchange for their services are not transparent, this may raise suspicions of corruption.

GOOD PRACTICES*

Ensure transparency of contractual agreements and payments made to host governments

- Make "a clear and unequivocal commitment to transparency of all revenue flows to governments. This should apply to every country in which a company operates." (CSBP, Flashpoint Issue 9: 6)
- Make all payments to governments available in company financial reviews and/or website, making sure figures are presented in a clear format. Guidance on related good practices can be found at www.publishwhatyoupay.org.

Work with host government authorities to increase transparency in the management of payments made by companies

- Assist in the development of a national financial reporting framework. Reporting frameworks need to be comprehensive and consistent for companies at the country level, and allow for proper analysis by civil society organisations and other observers.
- Work with other companies to promote common minimum standards for financial reporting.
- Cooperate with other companies to advocate for transparency of payments at the national level/with the host government.

Support programmes by governments, civil society and multilateral institutions to increase transparency in security sector financing

- Engage in multi-stakeholder processes such as the Extractive Industries Transparency Initiative at both the national and international levels. "This includes working collaboratively with home and host governments, international financial institutions, investors, civil society organisations, industry representative associations and other companies, including state-owned enterprises, toward ensuring that such initiatives evolve into meaningful and accountable standards of practice." (CSBP, Flashpoint Issue 9: 6)
- Seek ways to support security sector reform programmes that promote effective and accountable management of security budgets.

Inform communities about the company's actions

- Use booklets, video and audio that explain the companies' operational processes and payments in simple language. (CSBP, Flashpoint Issue 1: 6)
- Establish a public information office in a nearby location to the project site where anyone can make inquiries about the operations. (CSBP, Flashpoint Issue 1: 6)

GO BACK TO LIST OF CHALLENGES