The Voluntary Principles on Security and Human Rights

AN IMPLEMENTATION TOOLKIT FOR MAJOR PROJECT SITES

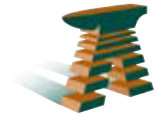
Multilateral Investment Guarantee Agency

Japan Environmental and Social Challenges Fund

In partnership with Anvil Mining

Working Paper — July 2008

World Bank Group
Multilateral Investment
Guarantee Agency



anvilmining

For further information, please contact:

Jill Shankleman
Deniz Baharoglu
Multilateral Investment Guarantee Agency (MIGA)
Environmental and Social Fund for Africa
1818 H Street, NW
Washington, DC 20433

t. 1.202.473.5244
jshankleman@worldbank.org

t. 1.202.458.9598
dbaharoglu@worldbank.org

This volume is based on the product of an independent author contracted through the Japan Environmental and Social Challenges Trust Fund executed by MIGA. The findings, interpretations, and conclusions expressed in this document do not necessarily reflect the views of the Executive Directors of the World Bank Group or the governments they represent.

About the author: Don McFetridge (BA, University of Texas; MA University of Hawaii; Senior Security Fellow, Fletcher School of Law And Diplomacy) retired in 2000 from a career in the US Army. He now works as a consultant on corporate security. His assignments have included working on security and business continuity for private sector clients developing major projects in Africa and Asia. His experience includes implementation of the Voluntary Principles of Security and Human Rights at the strategic and site level. Lee Nehring and Jill Shankleman also contributed to the document.

As a member of the World Bank Group, MIGA's mission is to promote foreign direct investment into developing countries to help support economic growth, reduce poverty, and improve people's lives. For more information about MIGA, visit www.miga.org.

The Voluntary Principles on Security and Human Rights

AN IMPLEMENTATION TOOLKIT FOR MAJOR PROJECT SITES

This page intentionally left blank.

Executive Summary

Investors in large-scale projects, particularly in the extractive industries, face the difficult challenge of how to safeguard company personnel and property in a way that respects human rights and the security of local communities. In a range of countries companies have faced allegations of human rights abuse related to security incidents where employees or other civilians have been killed or injured. In December 2000, the United States and United Kingdom governments, along with a group of extractive companies and non-governmental organizations, agreed on a set of principles, known as the *Voluntary Principles on Security and Human Rights* (VPSHR), to guide companies on security and human rights. The VPSHR provide a short, concise outline of actions companies should take to assess risks and implement public and private security measures in a manner that respects human rights.

Since the VPSHR were agreed upon, companies have accumulated considerable experience on their implementation. This document aims to make such experience available to security professionals, community relations managers and senior corporate management teams.

This toolkit on implementation of the *Voluntary Principles on Security and Human Rights* is a by-product of a project undertaken by MIGA's Japan Social and Environmental Challenges Fund for Africa[1] in collaboration with one of MIGA's client companies, Anvil Mining Ltd., to develop a comprehensive VPSHR implementation program for Anvil's operations in Africa. The tools and information generated during that project are now available to a wider audience. This document outlines how to develop and implement a VPSHR plan and how to gain senior management buy-in along the way. It would be impractical to provide a definitive, complete recipe book for compliance in all situations; rather, this document is a starting point for companies and projects to develop site-level VPSHR implementation plans tailored to their specific location and needs.

A security consultant who led the collaboration between MIGA and Anvil Mining was the primary author of this report, with contributions from MIGA and Anvil. During the initial study on which this document is based, the company staff, members of government security forces, residents and leaders of local communities and others provided valuable insights through interviews and other feedback. During the preparation of this document, specialists from the mining industry, non-governmental organizations and the World Bank Group reviewed drafts and contributed helpful input.

Readers should note that this document does not constitute official guidance either from the World Bank Group or from the VPSHR secretariat. Further, the secretariat of the VPSHR is currently developing formal recommendations for VPSHR implementation.

---

1 The Multilateral Investment Guarantee Agency (MIGA), a member of the World Bank Group, promotes foreign direct investment into emerging economies to support economic growth, reduce poverty, and improve people's lives. MIGA provides political risk insurance for socially and environmentally friendly foreign direct investments, offering protection against noncommercial risks such as currency inconvertibility and transfer restrictions; expropriation; war and civil disturbance; and breach of contract. MIGA also provides dispute resolution services for guaranteed investments to prevent disputes from escalating and keep investments and their benefits on track. In January 2007, MIGA launched a trust fund to provide technical advice to overseas investors in Africa. Through the trust fund, supported by a grant from the Japanese government, investors can receive expert advice from MIGA and from specialist consultants hired by the fund. The goal is to ensure that investments comply with or exceed MIGA's environmental and social policies.

THE VOLUNTARY PRINCIPLES ON SECURITY AND HUMAN RIGHTS

In December 2000, a group of six extractive companies, seven non-governmental organizations, and representatives of the U.S. and U.K. governments (Department of State and Foreign Office respectively) announced agreement on a set of voluntary principles (the VPSHR) to assist oil, gas and mining companies in providing the necessary security for their operations consistent with the promotion and protection of human rights.[2] The particular focus of the VPSHR is on the interaction of security systems and providers with the communities near extractive activities.

The principles are in three categories covering:

- Risk assessment,
- Relations between extractive companies and public security, i.e. police, military, etc.,
- Relations with private security contractors hired by companies to protect their facilities and operations.

For each, the text provides both general and more specific principles. The full text of the VPSHR is shown as Appendix 1.

Since then additional companies, NGOs and governments have adopted the VPSHR. These organizations have committed to improving security and human rights performance by sharing information through a series of plenary meetings and through the VPSHR website. Some of the companies participating in the VPSHR process have made documents related to VPSHR implementation publicly available. (See Appendix 2.) In 2007, the organizations involved agreed on formal criteria for participation in the VPSHR process. These criteria set out the obligations of participants in the process and acknowledged the need for consensus among existing participants in regard to new members. This information is available on the VPSHR website.[3]

Alongside the development of the VPSHR process, the principles themselves have taken on a life of their own. The principles have been adopted or have heavily influenced standards, policies and behavior of other organizations that are not part of the VPSHR process. In particular, the World Bank Group determined in 2004 as part of the Extractive Industries Review that the extractive projects it supports should operate in line with the VPSHR,[4] The Environmental and Social Performance Standards (PS) adopted over 2006/7 by MIGA, the IFC and the Equator Banks (which apply to projects supported by these organizations) incorporate the key content of the principles in *Performance Standard 4: Community Health, Safety and Security*[5] (See Appendix 3.) Companies that are not part of the VPSHR process, but which have decided to apply the principles to their management of security, often describe this as 'committing to apply' the VPSHR.

This report is addressed primarily to companies seeking to apply the VPSHR at an operational level.

Why apply the VPSHR? Companies that accept the responsibility of implementing the VPSHR do so for a variety of reasons: mainly to better manage security-related risks, to improve performance and reputation, and to comply with the requirements of financial institutions, project partners or shareholders. Many companies have concluded the VPSHR confer tangible security benefits to their facilities and to

---

2 For a list of original and current participants, see the website maintained by the Secretariat of the VPSHR at *www.voluntaryprinciples.org*

3 See *www.voluntaryprinciples.org*

4 World Bank Group Management Response to the Extractive Industries Review, September 2004

5 For the text of the full set of Social and Environmental Performance Standards and associated Guidelines, see *www.miga.org*. For discussion of the Equator Principles see *www.equator-principles.com*

the societies where those companies operate. Effective implementation of the VPSHR demonstrates a company's efforts to follow an ethical path when operating in host nations where the rule of law and respect for human rights are weak.

THE SIX SECTIONS OF THIS DOCUMENT

Section I outlines a process that companies might adopt to develop a VPSHR implementation plan and to integrate the VPSHR into company management systems. This is based on the work done through MIGA's trust fund with Anvil Mining. It outlines a phased work plan that begins with assessing and defining the status of VPSHR in the company at the beginning of the project.

Section II addresses the risk-assessment elements of the VPSHR. The VPSHR expand the scope of what is conventionally covered in a company security risk assessment to include community impacts and human rights risks. In particular, this requires that companies:

- Understand the potential for violent conflict in the area of operations,
- Assess risks to the community related to the company's presence,
- Develop methods to manage allegations of human rights abuse by public security forces within the expectations of the VPSHR,
- Evaluate risks associated with equipment transfer, e.g., what is appropriate for transfer and what controls are feasible to prevent misuse or diversion.

Section III addresses relations with public security services. Host-country public security forces are often under-staffed, frequently ill-equipped and have limited professional training. This section discusses ways a company can influence the deployment of the public security forces in relation to private sector projects, assist in setting expected standards for their behavior, help to develop rules of engagement for the use of force and arrange training on selected, non-lethal methods. It also discusses ways to receive and handle allegations of human rights abuse.

Section IV considers relations with private security providers. A company has much greater control over their private guard service than many other elements of the security system, because the company can specify standards of behavior in the contract. Section IV notes three challenges that require the company's attention with regard to its private security providers:

- Defining clear standards, performance objectives and deliverables,
- Assuring quality control though inspection, review and audit,
- Communicating the performance standards to the other security stakeholders.

Section V considers stakeholder engagement. Stakeholder understanding and support of the company's efforts to manage security and human rights risks is an integral component of the VPSHR. This section identifies the key stakeholder groups typical of major projects, and provides suggestions on engagement strategies and processes.

Section VI discusses integration of the VPSHR into the management system of an extractive company. The VPSHR have little value unless they become part of the company's corporate culture. Company leadership should adopt the Voluntary Principles and align the company's operations with them. This section outlines a phased approach to integration:

- Phase One specifies the highest-priority actions for company senior management to take in the short term, six months or less. In this phase, senior corporate management must take the initiative and show their resolve to apply the VPs.
- Phase Two includes a number of management actions needed to embed the VPSHR in the company. This phase focuses on building the interface between the community and host government, providing the resources to sustain engagement with stakeholders, and negotiating policies and protocols.

- Phase Three will see the VPSHR fully integrated into the “Company Way of Doing Business”. Management demonstrates this in tangible ways by: making the VPSHR a core value of the company; communicating the standards and expectations to employees; establishing the mechanism to deliver VPSHR implementation and performance metrics; and effectively reporting progress transparently to both the internal and external audience.

The appendices to the document include the full text of the VPSHR; the security sections of IFC/MIGA/Equator Bank Performance Standard 4 on Community Health, Safety and Security; a tool for tracking VPSHR implementation, and an annotated set of references and links.

Developing an Implementation Plan

This section outlines the approach, tools and outputs of a project jointly sponsored by MIGA's Japan Africa Trust Fund and one of MIGA's clients, Anvil Mining Ltd., to develop a systematic plan for implementation of the Voluntary Principles on Security and Human Rights for a mining company operating in a post-conflict African country. It describes one way companies can develop their own VPSHR implementation plan. The process described here was developed in the context of one particular company; some adjustments may be necessary to apply it to other companies or locations.

1.1 PHASED APPROACH

This VPSHR implementation plan followed a phased work program as follows:

1. Refine the scope of the study,
2. Conduct a diagnostic field visit,
3. Develop the implementation plan,
4. Review and adopt the plan,
5. Follow up and monitor progress.

Phases 1 to 4 were completed during a nine-month period. The company will follow up and monitor VPSHR implementation through the lifetime of the mine.

1.2 REFINE THE SCOPE OF THE STUDY

One key issue at the initial stage of the project was to decide whether to develop the VPSHR implementation plan 'top down' or 'bottom up', i.e., starting from a review of corporate systems and working down to the mine level, or vice versa. This study used a 'bottom up' approach because the priority, in this case, was to ensure that site-level performance was consistent with MIGA policies. In addition, the implementation plan was designed for a mid-size mining company with a small corporate organization and only a few operational sites.

The second focusing decision concerned the type of specialist expertise needed. In the eight years since the VPSHR were defined, a range of consultants and NGOs have developed the capacity to provide advice and support on VPSHR implementation. Some focus mainly on integrating the VPSHR into corporate policies and management systems, some on the community-interaction aspects of the VPSHR, and some on site-level security. For this project, the consultant selected was a security professional with site-level experience in integrating the VPSHR into site management of security and community relations. This choice reflected the project's initial focus on site-level implementation of the VPSHR. The company using the implementation plan had an existing relationship with an experienced local non-governmental organization. This NGO has experience with the VPSHR and is already providing some support on community relations.

The third aspect of refining the scope of work was to draft clear terms of reference for the consultancy, including a definition of what support and involvement the company would have and what relevant documents it would provide to the consultant for review. As an example, the terms developed for the MIGA project follow.

Consultant's Tasks

At the site level, the diagnostic study and associated recommendations will:

- Review and document how the company implements and monitors progress and results with respect to each of the specific commitments embodied in the Voluntary Principles;
- Review the effectiveness of the interface between community relations and security, and the mechanisms for regular consultation with communities. Propose how community recommendations can be incorporated, particularly in site-level action plans, and how communities can be engaged on an ongoing basis;
- Outline how the company, along with its contract security forces, can achieve its VPSHR commitments.

At the corporate and national level, building on the site-level findings, the scope of the diagnostic study and associated recommendations on priority actions over the next three years will include:

- The company's engagement on security and human rights with other companies, governments and civil society, including national and international NGOs;
- The company's support for initiatives by government, civil society and others on training public security forces and on building public institutions that are accountable and respectful of human rights;
- The company's corporate polices, processes, responsibilities and accountabilities to reinforce management accountability for implementation of the VPSHR at the site, national and corporate levels;
- Corporate procedures for handling credible allegations of human rights abuses by public security to the appropriate government authorities;
- Company policies on the use of its property by public security forces.

Company role and responsibilities:

- Liaise with the consultant to develop a detailed work plan, and manage the execution of the project.
- Provide access to the documents, personnel (staff and contractors) and sites necessary to enable the consultant to undertake the study.
- Identify senior managers at each level to act as primary contacts for the consultant, and ensure that these managers are available to work with the consultant to meet the needs of the company.

1.3 CONDUCT A DIAGNOSTIC FIELD VISIT

An initial assessment is essential to develop a good VPSHR implementation plan. Key points include: the context in which a site operates, the status of its security systems, the extent to which existing arrangements are compliant with the VPSHR, and the openness of security services to the approaches embodied in the VPSHR.

The diagnostic field visit for the MIGA project involved a two-week visit to the site that was the initial focus of the study. During the field visit, the consultant held meetings with company managers and staff, security contractors, local representatives of public security and intelligence forces, community leaders and locally based NGOs with an interest in human rights. In addition, the diagnostic visit included a tour of the site and surrounding area to understand the local geography and provide a context for understanding security and human rights risks.

During the field visit, the consultant gathered information on the national and corporate-level systems and resources for VPSHR implementation. This process included face-to-face and telephone interviews. The resulting assessment of VPSHR implementation used a scored matrix to illustrate the findings.

This matrix listed each element of the VPSHR with comments on the current implementation status at the time of the field visit. The consultant evaluated each component and assigned a color-code score: green for 'in place'; yellow for 'more work needed', or red for 'insufficient'. The consultant then

provided briefings to the client with the resulting diagnostic findings for their subsequent prioritization of tasks in the implementation action plan.

The diagnostic matrix framework, which can also be used to track VPSHR implementation over time, is shown in Appendix 4.

1.4 DEVELOP VPSHR IMPLEMENTATION PLAN

The implementation plan addresses the items identified in the diagnostic matrix as yellow or red, i.e. needing more work or insufficient. For each item, the plan provides a discussion of the relevant elements of the VPSHR. The plan outlines a proposed approach to address the issue and discusses the advantages and potential barriers to the recommended approach. The report also draws on short case examples to illustrate key points. Each recommendation includes a discussion of the resource implications of the implementation plan and a checklist showing a proposed phasing of actions.

1.5 REVIEW AND ADOPT THE PLAN

A consultant's recommendations are only useful if the client accepts and implements the recommendations. An important element of the process of developing the VPSHR implementation plan is to secure buy-in by company staff. The recommended approach is:

- To conduct workshops and meetings with company security, community relations and mine management staff and their external collaborators outlining the result of the diagnostic assessment,
- To solicit input into the conclusions, definition and timing of specific recommendations,
- To review the revised action plan with senior corporate management, focusing on the resource implications.

1.6 FOLLOW-UP AND MONITORING

Effective implementation requires ongoing evaluation and calibration. A company that has an active VPSHR program should present annual reports on the progress of the implementation plan. Through the initial period, the company can manage this through its own review process. During the VPSHR implementation program, the company should remain open and transparent, sharing experiences and lessons learned with other like-minded companies and security stakeholders. Each of these parties will play an informal role in monitoring the plan's progress.

However, at some point, an external review and assessment by an internationally respected organization is highly desirable. This review would be a good capstone event at the end of the three-year phased implementation plan. The company should expect to disclose the results of external review in the normal course of events.

Risk Assessment

Risk Assessment ensures the company has accounted for all foreseeable threats so that effective mitigation measures can be developed. This section examines the expectations enumerated in the VPSHR relating to the Risk Assessment (RA) component of the VPSHR, except those elements concerning Stakeholder Consultations. This section of the discussion also highlights some additional actions and processes that will assist in the implementation of the RA. That part of the RA concerning Stakeholder Engagement is addressed in Section VI.

Risk Assessment is one of the three key elements of the VPSHR. As there is no accepted industry-wide standard for Risk Assessments, the exact format and methodology are open to challenge. Therefore, the company must have a written formal process to maintain the credibility of the process. A Threat Register and Mission Essential Vulnerability Assessment will validate the assumptions that are necessary for a useful Risk Assessment. They frame the issues in a clear way for both security professionals and company management.

2.1 KEY TOOLS

The Risk Assessment process has many variations.[1] Many corporations have established their own procedural guidance for conducting a Risk Assessment. Essentially, any useful Risk Assessment is one that catalogs all known threats and evaluates their likelihood to occur and their potential impacts. Contingencies can then be planned to contain or protect against the consequences. Risk managers often use this basic methodology to assess a range of safety, environmental and even business risks to a project.

Two supporting procedures for Risk Assessments that are not always included in the basic security RA process are the Threat Register and Mission Essential Vulnerability Assessment (MEVA). These tools are useful in verifying and validating the basic assumptions that underpin all RAs.

The Threat Register enumerates all realistic threats. It should include threats to the local society caused by the mine, as well as threats to the site from the local community (mirror imaging).

2.1.1 Threat Register

The Threat Register is a catalog list of potential threats to the asset. It describes each activity and defines the parameters for later analysis. The Register defines and categorizes threats, but does not consider cause, probability or severity of impact on the company's people, assets, business continuity or reputation. The Threat Register answers the question, "Did you consider possibilities X, Y and Z?"

The Threat Register will develop over time as new threats emerge, other threats merge and some threats even disappear. The table on the following page is one way to create a Threat Register. For the purposes of this Threat Register example, it is not important what causes civil unrest. It could be a natural disaster, an epidemic, criminal violence, civil war or external invasion.

---

1 For examples, refer to *Introduction to Security, 7th Ed,* Robert J. Fischer and Gion Green, published by Elsevier Butterworth-Heinemann, 480 pp., 2004. *Risk Analysis and the Security Survey, 3rd Ed.,* James F. Broder, 392 pp., 2006 BUTTERWORTH HEINEMANN, ISBN-13: 978-0-7506-7922-0 and ISBN-10: 0-7506-7922-0. General Security Risk Assessment Guideline, ASIS INTERNATIONAL GUIDELINES COMMISSION, ASIS International, 1625 Prince Street, Alexandria, Virginia 22314-2818 USA, *www.asisonline.org/guidelines/guidelines.htm.* A RESOURCE HANDBOOK on DOE TRANSPORTATION RISK ASSESSMENT, U.S. Department of Energy, Office of Environmental Management National Transportation Program, July 2002. A Google search of the internet will provide numerous additional examples.

Example of a Threat Register*

Threat/Hazard	Application Mode	Duration	Extent of Effects: Static/Dynamic	Mitigating and Exacerbating Conditions
Civil Unrest (fixed location or regional) Break down of law and order, local authorities unable or unwilling to restore calm.	Lawless groups, criminal gangs, refugee masses, panicky crowds that threaten business continuity and possibly the site.	Hours to days or even weeks	Road travel cut or severely threatened, re-supply and personnel movement by air only, radio and satellite linked communications at risk.	External assistance complicated by remote nature of the local site location, limited road infrastructure and air strips, few resources (communications, electricity and fuel supplies), limited government public security forces in the area.
Unauthorized Entry Forced or covert	Use of hand or power tools, weapons, or explosives to create a large opening, or operate an access point (such as a locked door), or use of false credentials to enter a building.	Minutes to hours, depending upon the intent.	If goal is to steal or destroy physical assets or compromise information, the initial effects are quick. But damage may be long lasting if the perpetrators intend to disrupt operations, take hostages or cause injury or death.	Standard physical security design should be the minimum mitigation measure. For critical processing functions other measures, like CCTVs or traffic flow that channels visitors past access control, aids in detection of this hazard.

* Adapted from Table 1-3 of U.S. Government Federal Emergency Management Agency's "Risk Management Series, Reference Manual, To Mitigate Potential Terrorist Attacks Against Buildings," FEMA 426, December 2003.

2.1.2 Mission Essential Vulnerability Assessment

The Mission Essential Vulnerability Assessment (MEVA) looks at each location and process at the facility, determines the degree that each is critical to business continuity and estimates the time required for reconstituting or replacing the asset. The MEVA helps identify physical security shortcomings. The MEVA is not a process that directly contributes to identifying potential human rights abuses. When performing a MEVA, begin by meeting each of the functional managers who are the most knowledgeable experts on the process and the vulnerability of the components. These functional managers can identify those components whose loss would have the greatest impact on production until the company repairs, rebuilds or reconstitutes them.

Example of a Mission Essential Vulnerability Assessment**

Criteria	1	2	3	4	5	Score
Asset Accessibility	Remote location, secure perimeter, armed guards, tightly controlled access	Fenced, guarded, controlled access	Controlled access, protected entry	Controlled access, unprotected entry	Open access, restricted parking	
Complexity	Only a trained specialist can damage or destroy the asset	Difficult but not impossible to damage	Difficult to identify easily damaged parts; destruction very difficult	Major damage easy to accomplish; total destruction is difficult	Obvious, easily destroyed components requiring total replacement	
Presence of Hazardous Materials	No hazardous materials present	Limited quantities, materials in secure location	Moderate quantities, strict control features	Large quantities, some control features	Large quantities, minimal control features	
Collateral Damage Potential	No risk	Low risk/limited to adjoining area or facilities	Moderate risk/limited to immediate area	Moderate risk within 1-mile radius	High risk within 1-mile radius	
Numbers of People at Location	0	1-3	3-4	4-10	11+	
Total						

**Adapted from Table 1-5 of US Government Federal Emergency Management Agency's "Risk Management Series, Reference Manual, To Mitigate Potential Terrorist Attacks Against Buildings," *FEMA 426*, December 2003.

Once the criticality of the equipment or activity is determined, the operations staff will estimate their ability to repair, replace or reconstitute the function. The number of personnel normally located at an asset location is another indicator of the cost to reconstitute the function. The more people working at a location, the more difficult it is to recreate that activity should the site suffer a catastrophic loss. Together these factors provide a ranking of the overall vulnerability of each asset. Scoring each row and totaling the score gives a rough indication of the value of the asset in relation to other locations on site. These scores help prioritize where the protective resources should go.

Once the Threat Register and MEVA are complete, the Risk Assessment process continues. Risk Assessment training will provide a good example of a standard RA process. The analysis of each threat determines the likelihood that the threat will occur and the MEVA allows an informed assessment of the impact. The MEVA, and indeed the entire Risk Assessment process, is useless if management does not act promptly on the recommendations.

2.1.3 Recommendations

1. If there is no existing Risk Assessment, the security manager should perform one immediately.
2. Using the Risk Assessment methodology described in FEMA 426, review the Threat Register and MEVA[2] process. Conduct a MEVA and list the threats in a Register.
3. Verify the threats listed in any previous RAs that the company may have on file and any newly identified potential threats, including those indirectly caused by the company's operations.
4. Reassess the risks at each site using the new criteria for vulnerability to verify that the current RA remains valid for each component.

Advantages

- A review of all possible threats through a Threat Register will identify all potential threats and allow the company to address these through the RA process.
- Additional analysis and documentation of the vulnerability of the site's operational processes will help sensitize management to the degree of risk they have accepted (possibly unwittingly) without mitigation. For those outside the security hierarchy, this analytical product will underscore the importance of the full risk assessment process and the critical importance of effective mitigation plans.
- Solid planning, based on a comprehensive Risk Assessment, will minimize the dangers not only to the company's operations, but to the local communities as well. This establishes the best possible standard for an extractive industry operating in an austere, remote and underdeveloped location.

Scenario 1: Artisanal Miners

A rioting group of artisanal miners gained access to a large extractive complex. They took control of the mine's heavy equipment park and gained access to several large excavators and dump trucks. Although they were able to damage some equipment, they lacked the knowledge to start and drive the large machinery. The vehicles were not secured or disabled; the rioters could easily have used them to cause major damage. The mine's process control room with its computers and critical control equipment was nearby and at the mercy of the rioters. Had even one rioter known how to start one of the large dump trucks and then drive it through the control room, the site would have been out of operation for months at a loss of hundreds of millions of dollars. The complexity of the equipment and ignorance of the critical nature of the control room is all that saved the site from catastrophe.

For Discussion

Has the company conducted a MEVA at site?

Implementation Risks and Mitigation

- Adding additional steps to a complicated process may be too bureaucratic. One method of managing the MEVA and Threat Register processes is through a joint activity of the security and community relations departments. Once completed, the security department need only update the MEVA annually, or if there is a significant change in the facility. In contrast, the security manager should review and update the Threat Register monthly. This takes little time, but does require a disciplined approach.
- More "process" requires additional training and time for the participants. The additional time, however, will not be significant.

Resources

The security manager should have the experience and skills to conduct these aspects of the risk assessment. The security manager may require some additional coaching or self-study to conduct the MEVA and produce the Threat Register. The company's functional managers and the logistics chief provide essential information for the MEVA.

---

2 The Vulnerability Assessment process in the FEMA Guide does use the terminology MEVA, but the Vulnerability Assessment process is essentially the same thing.

2.2 ASSESSING RISKS TO THE COMMUNITY

The Introduction to the Voluntary Principles focuses attention on the impacts that company operations may have on the security and human rights of the local community:

"Taking note of the effect that companies' activities may have on local communities, we recognize the value of engaging with civil society and host and home governments to contribute to the welfare of the local community while mitigating any potential for conflict where possible…"

2.2.1 Discussion

The Risk Assessment process many companies use has traditionally focused on threats *to* the company rather than threats *caused by* the company. Many RAs done by and for companies do not address this issue. The RA should include threats to the local society generated by the normal activity of the company. This is a process of mirror imaging. Company operations can *unwittingly generate threats* from the community that then disrupt business continuity. The VPSHR notes "that companies' activities may have [an effect] on local communities..." As such, and in the interest of transparency and thoroughness, bringing the local community into the Risk Assessment process is wise. While the specific focus of the VPSHR is to bring communities into the discussion of security and human rights issues, the best way to facilitate this is by addressing security across the spectrum. The best security asset is a strong community relations program.

Assessing the impact of operations on local communities is an important method for identifying potential causes of animosity that could lead to hostility in these communities. If local communities tilt away from trust and confidence in a company toward hostility and confrontation, the process is almost irreversible. Once an adversarial relationship develops, security and operational costs as well as outside criticism and reputational damage escalate dramatically. The court of public opinion is inclined to side with local societies over multi-national corporations in such cases. Damage control is exorbitantly expensive and rarely effective.

All of this argues for a Risk Assessment, conducted by skilled practitioners, that brings the concerns of local communities into the discussions.[3] This dialogue can generate better awareness among all parties of potential dangers. The process could also help community leaders understand their own roles in taking ownership of some mitigation measures. Community involvement in risk assessment will raise confidence that the company is fully aware of their operational impact. The company cannot make the assumption it entirely knows and fully understands these effects.

Some activities have an impact that may not initially seem related to security, but later evolve into a security issue. For example, project-related traffic is often underestimated as a source of security incidents. Heavy truck traffic on a local road is an obvious safety concern. Company trucks using such roads on a continuing basis can inflame the local community. It is likely the company is cognizant of the danger posed by their truck traffic and may have mitigated this risk with speed bumps and reduced speed-limit signs at village entrances.

Speed and safety are not the only threats from traffic. The local roadside communities may identify additional concerns associated with the vehicles, even if there are no traffic accidents along the road. Beyond safety, the traffic is also a health issue as dust coats foodstuffs laid out for consumption or sale along the road. Dust will quickly cover laundry hung to dry, food in preparation and cooking utensils. In

---

3 The issue of community representation and methodology is a complex one. This is one reason a skilled practitioner of the process rather than an untrained executive is a better solution to conduct this dialogue. Even respected local nationals may not have the mediation skills to avoid getting enmeshed in unintended commitments.

addition to speed bumps, the company can take a number of other steps to reduce this negative impact including:

- Working with the affected communities on ways to mutually manage the issue,
- Adding additional, closely spaced speed bumps or rumble strips, sidewalks, etc.,
- Erecting safety billboards along the route,
- sending a water truck ahead of product convoys to dampen the dust,
- Using "Drive Smart®" or similar technology to record vehicle speed and location,
- Using only designated times for convoys that avoid periods of high activity in the villages,
- Disseminating the movement schedule so villages can avoid hanging laundry or preparing food at these times, etc.

The community can work with the company to design measures that are effective without unduly hampering the company's operations.[4] Failure to address this issue effectively could result in unilateral community action, such as erecting roadblocks or obstructions, staging protest demonstrations or making other demands that put the company on the defensive and draw in the police or others to resolve the dispute.

Companies should also be aware of indirect impacts of their operation. For instance, successful commercial activity attracts opportunists, vagabonds, unemployed individuals and others to the area. Local communities may not foresee the possible downside of an influx of new arrivals. Newcomers may have technical skills the locals do not possess, such as language fluency, education, heavy equipment experience, vehicle driving, etc.

These attributes make the newcomers attractive to the employers – not only the company, but also local sub-contractors who may operate without much regard for social responsibility or VPSHR expectations. The influx of these migrant laborers looking for work at the site may undermine existing traditional social control mechanisms and undercut the traditional leaders of the society. Inflation caused by the influx of wages and large

Scenario 2: Failure to Involve the Local Community

A logging company working in a remote location requested the police to send a detachment to their site to safeguard operations. Over time, the five policemen assigned abused local residents who were intimidated and afraid to report the abuse. In circumstances still not entirely clear, the five policemen were attacked and killed and their weapons taken by persons unknown. A company of riot police, outraged at the deaths of their compatriots, then stormed into the village torturing and abusing scores of people. Reports by NGOs indicated the police killed over a dozen people in an attempt to recover the weapons and identify the culprits. They failed to do either. This became a notorious case internationally, embarrassing the government, the police and the logging company. The company had not considered it had any responsibility to protect the community from the police it had brought in to protect their operations. The police antagonized the local community, but the problem started when the company ignored the negative impact of their operations on local livelihoods and social order. Further, the police normally did not operate in that local area. Their presence was uninvited and their actions unexpected by the community. The area police commander left this small, poorly led detachment without support. Their lack of discipline eventually led to their deaths and the deaths of others.

For Discussion

What responsibility do companies have to assess risks and mitigate consequences to communities from government security forces?

4 There is scope as well to consult with experienced NGOs on what best practices may have been useful elsewhere. In addition, the local police may be able to help with traffic control at high-risk locations.

numbers of newcomers, some of whom are likely to be predatory or criminal, will destabilize the local communities. This fuels a downward spiral in law and order, increases the vulnerability of company operations (especially outside the site perimeter) and marginalizes the original populace.

2.2.2 Recommendations

1. Using the Risk Assessment methodology, conduct an Impact Assessment of the company's operations with local leaders and opinion makers in the community. Identify community concerns and explore mitigation measures.
2. Expand this dialogue to include public security forces and local government when appropriate.
3. Enter any threats identified into the company's Threat Register.

Advantages

- Spreading the consultation and discussion to the local community involves all parties in identifying issues and developing solutions.
- This process will open the security dialogue with those concerned and demonstrate that "the company listens as well as talks". In so doing, the company reinforces the concept that all parties share responsibility and will manage issues jointly.
- The company's consultations with the local community can establish a mutually beneficial relationship of equals, versus a client-and-patron relationship.
- Collective consideration of issues can build problem-solving capacity in local communities.

Implementation Risks and Mitigation

- Public consultations can raise expectations in the community if they are not carefully planned and conducted. In any case, public consultations are necessary. An organized and coordinated approach is the only realistic, effective way to manage the issues.
- Community action in response to perceived threats, such as unwanted in-migration, may take vigilante form. Effective security consultations are the optimum way to address this. While this is a relatively rare development, the key is for the company to recognize that its operations have negative as well as positive consequences. The company should identify and pre-empt such negative developments in order to mitigate and manage the problems that will surely lead to greater trouble.
- The company can be accused of using community consultations to shift responsibility for its actions to others (i.e. hire newcomers and then disavow the consequences). Strict enforcement of contractual agreements with all contractors and making the hiring and training processes transparent will mitigate this potential problem. The company should constantly reinforce its key message – "Local hiring is done fairly and openly" – and ensure that locally appropriate ways are found of making hiring fair and open. Local unemployed persons will be suspicious and can easily become hostile and confrontational. Community liaison officers should be particularly alert for signs of discontent and report these indicators. This will allow the company to try and address the issue quickly.

Resources

Assessing the risks to the community will be part of the overall risk assessment process. This will entail negligible additional time or other resources.

2.3 POTENTIAL FOR VIOLENCE

The VPSHR state:

"Depending on the environment, violence can be widespread or limited to particular regions, and it can develop with little or no warning. The company should consult civil society, home and host government representatives, and other sources to identify risks presented by the potential for violence. Risk assessments should examine patterns of violence in areas of company operations for educational, predictive, and preventative purposes."

Any analysis of the potential for violence involving the company and the community is delicate. Both the company and the community have legitimate concerns about acknowledging that such a potential exists at all. For the company, this could imply that either the company is irresponsible, or it is unable to manage its relations with the community. The community will be similarly reluctant to admit the risk of violence targeted at the company or the government from groups in the community.

There are several sources of possible violence, including:
- Violence directly related to ongoing or recent civil conflict,
- Violence generated from within the workforce,
- Violence between the community and the government including its security forces,
- Violence arising from the destabilizing effects of uneven economic change.

2.3.1 Assessing the Potential for Violence

One effective way to calibrate the threat of community-based violence is at a company Security Committee Review. The core participants of the Security Committee should be the senior site manager, the security manager and the community relations manager. Others from the management team may attend at the discretion of the senior site manager. A small group is usually more effective, although where the senior management team comprises expatriates, it is important to ensure that the knowledge held by local staff is incorporated.

One way to ensure this committee remains effective is to schedule meetings immediately before or after the regular operations meeting. The committee is the place the security and community relations managers provide their insight and assessment of current conditions in the company operations area (this would include the immediate area of the site or facility, critical infrastructure such as the roads and the transportation network and other key sites). This meeting provides the essential verification that all parties understand the current social dynamic as it relates to security. The participants can then identify needed mitigation measures and take appropriate action. Managing complex problems on an *ad hoc*, as-required basis is usually ineffective.

The senior site management person present will drive the process by asking these key questions:
- Have conditions changed in the community for better or worse since our last meeting?
- Are there any new developments that the company should know about?
- Where are the next trouble spots likely to be?
- What should the company do to address the issues before they become a problem?
- When and how is our next issue likely to develop?
- What more is needed to protect the site?
- What are the company's responsibilities to the community?

It is possible that an unexpected event will surprise management. It is never permissible for the security or community relations departments to know about an issue and not communicate it to management for analysis and action.

In assessing the risk associated with violent behavior, the company cannot afford to become complacent in its routine operations. This means continued vigilance, monitoring and analysis of the potential for violence at the site and in the areas that could pose a danger to the site and the surrounding communities.

A confidential tracking system is a useful management tool for those on site, at company headquarters and beyond. This working document facilitates the assessment and reporting process. It also gives management a way to monitor trends and sharpens the focus of any required response. The Security Committee looks at each area and key function systematically every week, but normally need only submit it to senior management monthly. This tracking system should remain confidential because it is a subjective assessment. The report is sensitive; management should not share it with government authorities who may misuse the information. The system highlights sensitive areas. While intended as a site report, individual locations may require specific commentary if they are substantially different from the site as a whole.

Scenario 3: Workforce Violence

All too often, a company's management underestimates or overlooks its own employees as a source of inter-communal violence. The company's operations may be the only significant economic activity in the local region. As such, the company's activities generate fierce competition for jobs.

In 2006, a major construction project began to run over-budget and over-schedule in a remote, economically depressed region of a developing country. In an effort to accelerate the building activity, the prime contractor greatly increased the local, unskilled labor force. This overloaded the support facilities, as well as the supervision and management capabilities of the contractor.

Local laborers were resentful of the outsiders and jealous of the better pay and benefits enjoyed by the higher skilled outside workers. Tension between local and non-local workers erupted into a riot between the two factions after a minor incident. The security guard force, mostly locals, joined the "home team" and attacked the non-local workers and supervisors. In the ensuing brawl, hundreds of people were injured, more than 100 sufficiently seriously as to require medical evacuation. Several of the injured were in critical condition near death. Eventually, the authorities called in heavy reinforcements of riot police and army special forces. Once order was restored many of the police and soldiers remained, at the project's expense, on site.

The project had indications of this dangerous situation from smaller precursor incidents, but failed to recognize the extent of the danger or take effective measures to address the problems. Already over-budget and past schedule, the contractor was disinclined to invest in better working and living conditions, training programs or other potentially effective mitigation measures. In addition to numerous other lessons, the fundamental mistake made by management was the failure to look at internally generated threats, anticipate trouble and prepare accordingly.

For Discussion

How could management have anticipated the potential risk of workforce violence? What mitigation measures are appropriate for your

Example of a Security Tracking Report

[DATE]

(This document is CONFIDENTIAL when complete and not for the public domain.)

RISK	RED: IMMEDIATE THREAT YELLOW: MEDIUM THREAT GREEN: LOW THREAT	PREPARATIONS ADDRESS CONCERNS		RED: INSUFFICENT YELLOW: NEEDS MORE WORK GREEN: IN PLACE
SITE	METRICS FOR ASSESSMENT	STATUS		PREPARATION
		Last Week	Current	
Company facilities	Work force morale. Ratio of local to non-local employees in the labor force is 50% or greater. Incident tracking.			
Local villages	Local traditional leader effective. Newcomers able to integrate into community.			
Other villages nearby	Traffic control measures in place. Jobs at site distributed fairly.			
Closest large town	Liaison with government regular and effective. Crime rate stable. NGOs operate freely.			
Transport associated facilities	Contingency plans in place, security SOPs coordinated with police. Communications with local government authorities good. Business recovery program if access blocked.			
Police	Police liaison ongoing. Police responsive to allegations.			
Military	Good communications with military and intelligence representatives.			
Outer area of interest (beyond Site Area of Operations)	Good information and situational awareness. Investigation processes.			

2.3.2 Recommendations

1. Include communal violence as an assessment issue during monthly site Security Committee Review.
2. Establish confidential tracking system to monitor and evaluate each location and critical function.

Advantages

- A tracking form focuses management attention and company resources to shape and manage potential hot spots.
- A regular tracking report helps reduce surprises, uncertainty and hesitancy to communicate concerns or bad news.

Implementation Risks and Mitigation

- Another form requires time and preparation. The best way to manage the time requirement is by careful preparation before the monthly Security Review. The company's security and community

relations departments are often already collecting the necessary information for other requirements. This process ensures dissemination of the information in a timely and coordinated way.

- Subjective assessments are always open to challenge. Over time, the demonstrated expertise of the security and community relations departments will reduce this. Skeptics, however, will always be with us and will undoubtedly challenge unsupported assertions. This is a good thing, allowing you to explain and validate the assessment rationale.
- An assessment could be compromised and enter the public domain. Close control of company confidential documents should already be in place and, if so, should be adequate to protect sensitive information. However, a well-developed assessment based on observable facts, ethical principles and historical experience will usually stand the test if exposed.

Resources
Time of site, security and community relations manager.

2.4 HUMAN RIGHTS RECORDS

2.4.1 Relevance to the VPSHR

The VPSHR include an expectation that companies will conduct an assessment of the human rights record of public security forces, law enforcement and security contractors in the host country. This assessment should focus on the historical and current performance of all state security forces. Such an assessment gives the company a realistic understanding of the operating environment and the risks it must mitigate.

2.4.2 Discussion

One significant challenge for a company in assessing human rights records is a paucity of reliable documentation concerning specific units and individuals. It is possible, however, to make a good-faith effort to check the background of individuals (a Pre-Employment Screening or PES) and the record of accomplishment of some units. Such documentation, when it exists, can be used to identify past human rights abuses. The company must use its influence to prevent those with records of human rights abuses from being involved in company activities, especially security activities.

The company has some implied responsibilities under the VPSHR when addressing the issue of human rights records. The first of these is to establish a clear understanding with the host government of the company's expectations concerning allegations of human rights abuse. The protocols between the company and the local and provincial government are an excellent way to accomplish this.

Next, the company should perform a credible PES investigation of those directly engaged in security and related activities, particularly those in supervisory positions. This is not simple in a developing nation where records are incomplete, especially where there is a history of official indifference and impunity. In some countries, there are internationally recognized and reputable security companies that specialize in political risk advice, investigations and security consultancy. Often such companies have the capability to do thorough background investigations that are beyond the scope of an industrial company's security department.

Absent other resources, the company can take the following steps to make a good-faith effort to determine the human rights record of those who may be providing security services, directly or indirectly, to the company:

- Conduct an official check of police records for any outstanding criminal warrants on prospective candidates.
- Check with appropriate embassies as to known or indicted human rights abusers. Note also that

the U.S. State Department Country Human Rights Report does mention some individuals by name as alleged human rights abusers or war criminals.

- Follow up with knowledgeable NGOs, including the churches, which may have knowledge of specific human rights allegations.

It is not necessary to make the results of these inquiries public. All information collected is sensitive and should be held in strictest confidence, filed under lock and key, and not attributed to any individual or organization. Mishandled or carelessly revealed information can pose a grave risk to individuals, not only from public security forces, but also from a range of actors in the community. If there is a challenge to the vetting process, it is sufficient to describe it as a deliberate effort to access the credible sources of such information. The company must be able to verify that it conducted an inquiry and took those steps that were appropriate and consistent with the expectations of the VPSHR. The company is not a human rights organization nor is it the investigative arm of the human rights community. However, the company will be held accountable for making every effort to ensure those with records of human rights abuse are not used to provide security services to the company.

If credible allegations do emerge concerning a specific unit or individual, the company is obligated to take note of this and request reassignment of the unit or individual away from company facilities. The company should request this discreetly, at a level appropriate to maintain confidentiality. If for whatever reason the authorities do not honor the request, then the company will take steps to closely monitor all activities of the unit or individual in the company's area of operations. Where possible, company personnel should accompany or observe the activities of the unit or individual when on company property. This permits the company to protect itself from future allegations of complicity, and potential legal action. Such monitoring is awkward and inconvenient. It can potentially be dangerous. It is all the more important therefore to pre-empt this risk if possible. If the worst happens, the company will immediately take action to report the allegations at the appropriate level to ensure the government initiates an investigation and takes disciplinary action where justified. (See 3.5, Responses to Human Rights Abuses.)

When a company, including its supporting activities and sub-contractors, brings in additional public security forces, that company becomes *de facto* responsible for the actions of those forces, at least in the public's perception. External events or pre-existing conditions may require the presence of these security forces. Regardless, the company inherits an obligation to be very careful about the process, to do a Risk Assessment of the impact of additional forces on the local community, to

Scenario 4: Failure to Evaluate Potential for Human Rights Abuses

In the midst of a period of serious armed rebellion, a multi-national corporation demanded protection for its operating location from the state public-security forces. Subsequent to this, the corporation provided support and assistance to the military forces deployed. NGO activists subsequently alleged that the host country's army used company property (a shipping container) as a torture chamber and a company bulldozer to dig a mass grave for victims of that torture and other arbitrary, extra-judicial executions. While the many details of the case remain obscure, the negative publicity has been a black eye for the corporation in the court of public opinion, both locally and internationally. There is no appeal of a conviction in that court. The incident has already entailed significant legal costs to the company, damaged its corporate reputation and discredited its procedures. Company management has not been able to establish that it maintained close and continuous monitoring of what happened at its facilities and with its equipment.

For Discussion

To what extent would prior evaluation of potential for human rights abuses have protected the company from these consequences?

identify and mitigate potential negative consequences, and to make the company's concerns clear to all security stakeholders. The company should also understand exactly what capabilities the additional public security forces bring to the situation. Often this is only additional manpower and lethal force.[5] In such cases, special monitoring is essential to protect all parties. The actions of the public security forces are under scrutiny at all times; they must understand that the company will promptly report any allegations of misbehavior.

2.4.3 Recommendations

1. Establish a procedure to investigate public security forces units and individuals to determine if there are credible allegations outstanding against them.
2. Make known through relevant protocols and other agreements what the company's standards are for ethical and moral conduct. Ensure all levels of government are aware of the VPSHR and the company's obligations to them.

Advantages

- The company informs all stakeholders about its concerns.
- The company's intent to maintain a dialogue on this issue is clear to all. Further, the company will show it intends to seek government support in shielding the company and its employees from suspect individuals or rogue units.
- These measures meet the company's obligations under the VPSHR to assess the human rights records of those specific individuals and units assigned to security operations in the company's area of operations.

Implementation Risks and Mitigation

- The company should handle this procedure at the appropriate level and with discretion to maintain confidentiality and protect those at risk from pressure or retaliation. Protection of the company's confidential materials will help to mitigate this concern.
- The assessment process is open to challenge and demands from activist NGOs to take a public confrontational position. The VPSHR do not require it, nor do other participants make such information public.

Resources

Assessing human rights records is a key part of the Risk Assessment process. The security manager, community relations manager and legal counsel collectively make this assessment.

2.5 RULE OF LAW

2.5.1 Relevance to the VPSHR

In most cases, the company is governed by the host nation's legal system. Therefore, the company must determine the effectiveness and reliability of the rule of law with respect to its commercial and contractual relationships. The company must apply this diligence to determine the effectiveness of the legal system as it relates to security and human rights – specifically, the capacity of the host country institutions to hold accountable those responsible for human rights violations.

2.5.2 Discussion

In working with the state authorities, it is important to have a solid legal basis for the discussions. The company can make a more compelling case for its position concerning the VPSHR and its security protocols with the government, if it knows what national laws are on the books that codify and protect

---

5 It may also bring in a chain-of-command unfamiliar with the company's mode of operation, standards and expectations. In such cases, a written Code of Conduct and Rules of Engagement for the newly arrived forces are extremely useful.

the rights of individuals. The company can use this as an opportunity to engage a prominent local university's law school to develop a short report detailing the relevant legal codes that concern human rights, labor rights, protection of the individual and any related legislation covering the rights of traditional societies. The relationship developed and the modest resources required could spur the further development of humanitarian law studies. Eventually, this relationship could serve the company well as a resource for impartial assessments. An independent university moderator could perform a valuable role in creating the Community Security Forum.

In the event that local institutions of higher education lack capacity, it is usually possible to arrange internationally qualified subject-matter experts to participate in the effort. These experienced academicians from sister institutions in the European Union, North America, Australia and Japan are frequently eager to assist. Often international donors will assist this capacity-building process by jointly funding such cooperative arrangements or they can join separately with existing educational initiatives.

Alternatively, the company can establish contact with appropriate human rights lawyers or non-governmental organizations to get a summary of the relevant legal codes.

A check of donor countries will also reveal what programs are underway to strengthen the legal process, enhance court effectiveness and build the base of human rights case law. The company and others can best support the rule of law if they know in broad terms what the law actually says. It is in the company's

Scenario 5: Cooperative Programs with Local Universities

An international NGO developed a program of community-oriented policing in a major city that had experienced considerable distrust and friction between the police and the local community. Using a local university's legal department as the facilitator and catalyst, the NGO developed a program that strengthened the skill base of the university's faculty and students. The program lowered communal tensions in the city and enhanced the professionalism of the police. The national police chief hailed it as a model for other cities.

This concept was the basis for a similar program by an extractive project in a remote rural part of the country. The nearest university did not have a law school, but did have a faculty of social sciences. Its vice-rector found faculty resources in sociology, anthropology and business who took on the challenge. The company/university relationship blossomed.

When local workers could not pass literacy qualifications for employment in the security-guard force, the university developed an intensive three-week refresher to raise the skills of the locals to a passing level. The university also performed various census studies, opinion surveys, social assessments and served as a respected resource for the company, locally and internationally.

Throughout, the university kept its integrity and impartiality intact. The university, starved for funding from the state budget because of its remote location and limited facilities, benefited from the opportunity to show that it was capable of performing quality work despite its limitations. The arrangement allowed the university to offer greater opportunities for local students, otherwise closed off from higher education by virtue of their isolated location. This was an exceptional win-win relationship for all.

For Discussion

Are there opportunities for this approach in your company's areas of operations?

interests, and those of other similar companies, to support the efforts of national and international donors who have programs to strengthen and modernize the legal system in the host country. These agencies have the expertise, time and charter to help strengthen and reinforce a host country's legal system. More direct involvement by the company carries the danger that the company will be accused of trying to manipulate or influence the legal reform process to the company's advantage.

2.5.3 Recommendations

1. Establish a consultative arrangement (contract) with reputable local universities to undertake studies and projects of mutual interest. The first of these could be a survey of the country's ratification of international human rights conventions and of the relevant national laws that address human rights, labor rights, international humanitarian law, etc., with a summary of the key points in both English and the host country's national language. The company should set realistic expectations in scope and timing for the university.
2. Explore human rights programs sponsored by international donors to determine if there are opportunities to support such programs in the host country.

Advantages

- This initiative provides an additional resource that the company can use in a number of ways.
- It demonstrates support for the development of the rule of law and international humanitarian legal principles in the host country that aren't based on the company's philanthropic commitments.
- It can open the door to other opportunities where an impartial view enhances the credibility of the activity.

Implementation Risks and Mitigation

- The selected university may require some capacity building, especially if it has to access external resources. This commitment is likely to have greater resonance with local elites and a wider impact than other development programs. Many outstanding international universities are searching for ways to be relevant to the needs of developing countries and if approached would participate. Multi-party initiatives, through organizations of like-minded companies, can be effective in sharing the costs and generating expertise.
- A partnership with a university can be more expensive and time-consuming than using internal staff resources or a commercial contractor. This is situational and staff-dependent. More importantly, such studies are not a core business of most companies. Accordingly, the company is wise to outsource the service.

Resources

The extent of a contract with a local university or universities will depend on a number of variables and the extent of the work the company wants done. It is best for the company to start with a limited commitment and expand as the products and requirements dictate.

2.6 CONFLICT ANALYSIS

The company's effectiveness in implementing the VPSHR will depend on its understanding of its operating environment. This includes a full understanding of the potential for communal violence. This will allow the company to gauge the social "operative temperature" of the local society. Without this knowledge, any VPSHR risk assessment the company performs is unreliable.

An extractive company may find a limited range of resources to draw upon for its analysis of conflict in the host country. In particular, a recent history of conflict is likely to inhibit academic study. While the broad outlines of the conflict may be clear, local anthropological and sociological studies are often scarce. Few if any countries experiencing the recent boom in extractive activity have had an external strategic impact assessment. Companies rarely make such assessments and usually lack the trained personnel and expertise to do so. Therefore, the company usually begins with only anecdotal

evidence, local perceptions and some educated observations by knowledgeable observers. One key tool in conflict analysis is a Security and Human Rights Assessment.

2.6.1 Discussion

In such circumstances, it is appropriate for a company to undertake – on its own behalf or in collaboration with other operators – a Social and Human Rights Assessment, especially if a company expands its operations into multiple locations in the region. A qualified individual, company or NGO can perform this assessment. In many cases, a local university may have the skills and expertise in the anthropology or social sciences departments to undertake this study. The company should take the opportunity to map the ethnic, religious and social groups in its area(s) of operations. This process is useful to reveal both the dangers and the opportunities for the company as it builds its operations base and associated security system. It can reveal unexpected sources of conflict management in the society. Such studies identify real and nominal centers of power, influence and opinion. In traditional societies, especially those under stress and remote from other government institutions, such knowledge can mean the difference between success and failure for the company. The agency conducting the assessment should interview local public security forces as they normally have the responsibility for monitoring potential sources of internal conflict. Companies may elect to draw from more than one source for this information.

Assessment of the potential for conflict will also allow the company to identify vulnerable and potentially volatile key points (actions, events, people or activities) if social stability deteriorates. By monitoring these indicators, the company can initiate appropriate educational, preventive and protective measures. This approach to conflict resolution will involve all elements of company security, community relations and operations in a coherent strategy to deter violence – particularly violence directed against the company's activities.

Conflict analysis also will suggest what capabilities the company should deploy to manage the impact of conflict on its operations. If the company's best efforts to avoid conflict fail, and deterrence is ineffective, then adequate protective capabilities are essential to protect the site and the company's operations in the area.

2.6.2 Recommendations

1. Conduct a conflict analysis that includes a Social and Human Rights Assessment to identify and map sources of potential conflict. Commission a reputable local university, internationally respected individual or company to do this study.
2. Using the conflict analysis, identify observable key points that indicate that confrontation or violence directed against the company is likely or imminent.
3. Establish the means to monitor those key points.
4. Analyze the potential for, and degree of, conflict in the area of activities and develop a set of management strategies.

Advantages

- Conflict analysis clarifies the situation and provides tools for company management to assess the threat to its operations.
- Analysis identifies where the company's efforts should be concentrated to achieve its objective of safe and secure operations.
- The analytical process provides indicators that can assist the company's crisis management and decision-making processes, especially in determining what capabilities the company needs to maintain and support.

Implementation Risks and Mitigation

- Management and outside observers may misunderstand conflict analysis, seeing it as predicting,

rather than identifying, potential sources of conflict. Clarify the intent and boundaries at each stage of such studies.

- A Social and Human Rights Assessment may raise unwarranted or unrealistic expectations. Any study or statement is subject to misunderstanding and even deliberate distortion. Reputable human rights organizations and consultants with a proven record of accomplishment understand this and are careful to minimize this possibility.

2.7 EQUIPMENT TRANSFER

The VPSHR state that:

"Where Companies provide equipment (including lethal and non-lethal equipment) to public or private security, they should consider the risks of such transfers, any relevant export licensing requirements, and the feasibility of measures to mitigate foreseeable negative consequences."

Thus there is a clear expectation is that the company will only transfer equipment after the company has made a full assessment of the risks and has implemented appropriate mitigation measures.

Equipment transfer to government, public and private security forces is often unavoidable and usually controversial. The essential elements of concern when transferring equipment are: What is provided? Why it is needed? How it will be controlled and used? Who will get it and what degree of transparency is required? The company will be in the best position to manage this issue with a company policy that is realistic, flexible and open to scrutiny. In many cases, transfer of appropriate equipment and provision services in kind may have a significant positive effect on the human rights performance of public security forces. (Note: This section does not address transferring equipment to local communities. Such transfers *do* pose some concerns and can have negative consequences. However, the community relations department is usually the most appropriate agency to manage these issues.)

2.7.1 Discussion

A protocol with the relevant (usually local) government can provide for equipment, goods and services to government and public security forces. Even if this issue is managed at a higher level, local representatives will likely remain hopeful that the company will provide them with additional support, assistance and benefits. This is particularly true in areas where there are few amenities or public utilities and little budget to address pressing needs. The company should be prudent in extending support, but not shrink from doing so when necessary.

The ideal situation is to avoid direct transfer of equipment from the company to public security forces and government. Giving equipment, other than very specialized safety items required at a hazardous work site, poses challenges. The preferred way to ensure needed equipment is in the hands of the public security forces is to identify to the appropriate government agencies what equipment is required and insist the host government provide this material. In some cases, state agencies have agreed, as part of the overall contract of work with a company, to provide certain capabilities resourced from the taxes, royalties and revenues of the project. It may also be possible to set aside or earmark a percentage of the company's royalties for security and other local purposes. This could be especially effective if the company offers matching funds to a jointly managed contingency fund that can dispense the money for mutually agreed-upon requirements. Such funds would have to have strict accountability. Many local governments and public forces particularly find this an attractive procedure, because it circumvents cumbersome bureaucracy and provides dedicated funds directly to the intended recipient. In other cases, governments have allowed cost recovery of expenditures for support provided to public security forces. Either method allows the company to make sure public forces have the quantity and quality of equipment necessary to perform their duties without incurring the liability of training, maintenance, fuel and spare parts. Jointly administered funds also allow better control over the funds.

Another way to approach the issue is through international public-sector reform programs. Police reform and training programs are in place in many countries and include training as well as equipment transfer. The company may need to lobby these programs to extend the police reform activities to the area of the company's operations. If the efforts to get the host nation or bilateral donors to provide the material and support needed, the company can look to a collective approach through a grouping of concerned companies. Each company can contribute to a consolidated program of equipment and training that will jointly benefit all companies in the area. These approaches to the issue avoid entangling the company in concerns about improper influence of public officials. If these strategies fail to provide essential support to the police, then the company should evaluate the benefits of providing the resources necessary to give the public security forces viable methods to enforce the law and avoid human rights abuses.

As part of the Risk Assessment process, the company will identify various mitigation measures to address various threats. The company should decide how it expects to handle threats across the spectrum. The more situations the company's security guards can handle, the fewer issues that will require police intervention. The company has greater control over its contract security guards than over any assigned policeman. Therefore, it should provide them with the training and equipment necessary to perform the task of maintaining security in all situations that do not require a law enforcement official.

As part of that task analysis, the company should determine what capabilities it needs urgently and those it is likely to need in the future. The security program at many sites has only four capabilities:

- presence and deterrence,
- discussion and negotiation,
- unassisted physical force by the guards,
- lethal force by the police.

These capabilities do not cover the full spectrum of threat and do not offer a graduated response between shouting and shooting. If confronted by an unarmed, but violent threat such as a deranged individual, a drunken group of rowdies or even a mob, the guard force must accept the risk of serious bodily harm to perform its protective mission. A detailed analysis of the exact nature, quantity and control of additional security equipment is beyond the scope of work of this study.[6]

When the guard force cannot control an incident, the police will step in. In such a case, the only thing the police officer usually has that a guard does not have is a police weapon. The company should assume the policeman will use his weapon because that is all he has available. Therefore, the company should use extreme caution when summoning the police.

The same Risk Assessment and analysis should identify at what point an incident becomes a police issue. If that point is less than "clear threat to life and limb requiring the use of firearms", then the police must have capabilities to respond below that level. If the company decides to limit its contract guard force to a certain level of capability, it is incumbent on the company to ensure the police can address any threat above that level. This responsibility entails that the company work with police officials to determine what equipment capabilities are required, what the government can resource and what shortfall the company should address. The transfer of the required equipment can then proceed under

6 A number of protective and defensive items are likely to be appropriate. These include handcuffs, batons and safety helmets as basic issue. An assessment of the police capabilities may disclose the requirement for additional crowd control equipment, such as acoustic devices, sticky foam, pepper spray, protective shields and faceplates. Above all, the guards need the training and practice to build their confidence in themselves and their equipment to handle any contingency short of lethal force.

the caveats and guidelines above and with such training and safeguards as are possible. The police must agree that any equipment provided for the protection of the company, especially any items provided *by* the company, remain in place unless the police have the express permission of the company.

2.7.2 Managing Transfers

The VPSHR do not restrict or prohibit the transfer of equipment, including lethal equipment, to public or private security forces. The concern, however, is that the equipment is necessary, is appropriate and is controlled such that it will not be misused to cause human rights abuse.

In determining the risks associated with equipment transfers, the company should balance the positive benefits against the possible consequences. The more dangerous and potentially lethal an item is, the more cautious the company should be in providing it. Generally, the company should assess what capabilities are required and ensure those are present, even if it has to provide the needed equipment, training and support. For example, the police in many countries often only have their firearms, typically AK-47s, as their equipment for maintaining order.

If there is an incident that requires the police, the patrolman has only two strategies – shout or shoot. In this circumstance, the company may determine it is in the best interests of all concerned to make sure the local policeman has other alternatives. In the best case, the government should provide the required additional equipment (see above). If this is not possible, then the company may elect to provide the resources through a reputable private contractor. If this latter course of action is necessary, then the company should ask that, as a condition of the donation agreement, the government commit to respect human rights and the appropriate UN covenants and standards for the protection of individuals and the use of force. In many cases, the under-resourced law enforcement agencies will readily agree.

Scenario 6: Equipment Transfer

A project site was located some distance from the closest police station and civil authority. The police had neither their own transportation nor communications. The one-way trip to site took up to an hour and a half, once the police mobilized. To facilitate the response and cut the time for the police to arrive on site, the project provided a two-way radio, batteries and battery charger, and the transportation and operators for police response. In the event that the police made an arrest, the project provided an escort for the prisoner to make sure there was no abuse while en route to the station. All this was coordinated in pre-existing Standard Operating Procedures (SOPs). In this case, the project supplied equipment (the radio), support en route (the transport) and safeguards for the employment (escorts). While not perfect, this system met the security needs of the project by providing resources to the police in an appropriate way.

For Discussion

What can the company do to manage equipment transfer and ensure the company can monitor equipment to meet the expectation of the VPSHR?

Legal accountability is required to stay within the bounds of laws concerning corrupt practices in the host country and the company's home country. The company should 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.

The provision of equipment will also entail support costs. This sustainment support is essential. However, this sustainment burden is not without some benefit. It is usually possible to control the use, and discourage the misuse, of donated equipment through the control of maintenance, spare parts, fuel or other essential material. In some cases, it may be necessary to provide personnel, such as vehicle drivers, to operate the

equipment, which will allow even greater oversight of the intended employment of the equipment.

The same conditions and considerations are valid for transfer of equipment to private security guards. In most cases, however, the guard force can provide the equipment and training necessary to establish a required capability. For example, if the company determines it needs the local guards to be able to restrain a lawbreaker until the police can arrive and make a formal arrest, it can make this a required capability for the guard company. That contractor will then provide handcuffs or plastic restraints to the guards, train them in the use of restraints, caution them about the potential for misuse and supervise the employment. The same procedure might be necessary for deployment of non-lethal crowd-control items. The company should preclude the use of firearms for its contract guard force unless this is clearly unavoidable and justified by the Risk Assessment process.

2.7.3 Pay and Life-support Issues

If equipment transfer is controversial, providing per diem and life-support resources is even more sensitive. The VPSHR do not prohibit paying a per diem to police or other public security forces.[7] Indeed, it may be the only way to curb predatory behavior. In many countries, where the police have no other recourse to maintain themselves, the government may tacitly expect them to 'live off the land'. In such cases, if the company ensures the police at its facilities have proper living conditions, good food and health care then police morale and discipline generally improves, especially if the company makes its expectations known to the police commanders. The company will often find it has protected both its operations and the local populace from incidental inappropriate behavior of the public security forces.

The key to making this strategy work is full transparency. Anything less will inevitably encourage abuse.

2.7.4 Recommendations

1. Include equipment transfer in the Risk Mitigation measures and assess the risks involved with equipment transfer.
2. Recognize that lack of proper equipment increases the risk of inappropriate use of excessive force.
3. Establish the protocols for equipment transfer, control of the process, recognition of the associated training and support costs, methods to ensure transparency and engagement with the security stakeholders to clarify why transfers are necessary.

Advantages

- The security forces – public and private – will have the proper resources to meet the full spectrum of contingencies without prematurely resorting to lethal force.
- There is greater control over the equipment, reducing the opportunities for its misuse.
- Management has a greater range of options and methods to confront and manage security threats. The right equipment is on hand to handle problems in an appropriate way at the lowest threshold of engagement.
- Properly trained, equipped and led public security forces will be better prepared to perform without resorting to human rights abuse.

---

7 Paying for "call out" services is commonplace among police forces around the world, including advanced societies. Organizers of public events routinely pay off-duty police to perform security functions at the event. If the company operates a facility that requires police security that would not normally be deployed to that area, or in the numbers required to protect the company, then paying for such services is justified.

Implementation Risks and Their Mitigation

- There is always some chance of misappropriation or misuse of company-provided equipment. This is rare, however, and can be best managed by making the terms and conditions of use clear before the transfer.
- The recipients may use the process of equipment transfer to press for additional support or resources. These demands could include support and maintenance of the public security forces elsewhere. This is best managed by ensuring equipment transferred is simple, rugged, proven and easily supported by local craftsmen. In the case of advanced or complex equipment, a maintenance support contract should be included as part of the transfer agreement. Fuel and operating supplies should be included in the provision agreement or the transfer will be a waste of resources.

Resources

The company will list and monitor any equipment that it provides to the public security forces. This is a logistics function, with assistance from the security department. The cost of the equipment depends entirely on what the police need, what the company decides to provide, and on the maintenance, support and associated training required.

Relations with Public Security

Relations with public security forces are a major element of the VPSHR. In some countries, the host government mandates that public security forces are present at important, or vital, economic locations, including major industrial sites. Police in particular are normally a deterrent to public misconduct and criminal activities. Provided the company manages its relationship with the public forces properly, the company can have a positive influence on the host nation's respect for human rights far beyond the boundaries of the company's operations.

In the host country there will normally be three main components of the state's security forces that interact with the extractive industry: the police (including gendarmerie, specialized forces for mines, oil and chemical industry, border and coast guard, fiscal and customs, etc.), the military forces, and intelligence organizations. Each of these has challenges and limited resources. Often they are under-staffed, poorly equipped and have limited training. In many cases, these conditions may be the result of a long period of civil strife. The company should maintain appropriate contact with all these agencies and should have a clear, articulated and, within the bounds of confidentiality, an openly acknowledged policy of engagement.

3.1 COMPANY POLICY AND BASIC PRINCIPLES OF INTERACTION

The company should formulate its engagement strategy around these principles:

1. Avoid situations where intervention by public security is required – use the Job Safety and Security Analysis (JSSA) process.
2. Use company security first. Public security forces are the last resort. Never ask a member of the public security forces to do something if company security can legally do it.
3. Minimize the presence of public security forces at company sites; request public forces only when there is an urgent need at a specific location and then set time limits for their expected withdrawal.
4. Negotiate and sign protocols with the public security forces that clarify expectations and obligations of both parties.
5. Support the capacity-building efforts of public security forces in ways consistent with the VPSHR.

Deployment of public security forces to company facilities can have only three results, two of which are counter-productive: First, the public security forces take appropriate action to maintain law and order as expected – a good consequence. Second, the public security forces are ineffective and idle, taking up resources without making any useful contribution – not good for a number of obvious reasons. Or, third, the public security forces behave in an inappropriate way, causing unnecessary harm to the company or others – obviously very undesirable.

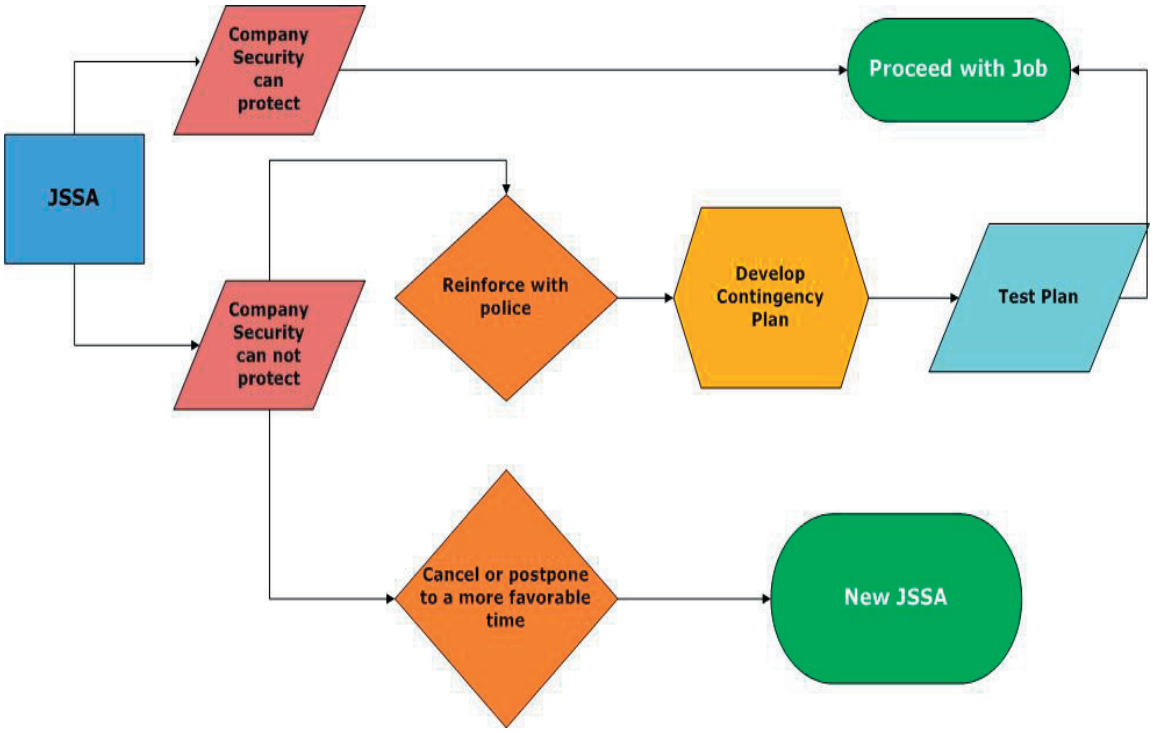
Consequently, the best utilization of public security forces is for them to perform their legitimate functions in maintenance of communal law, order, and defense of the nation and to remain vigilant at their normally assigned duty locations. This is especially important if the local communities experience a major influx of opportunity-seekers as a result of the company's activities. The way to avoid the undesirable second and third scenarios above is to implement a proactive, preventive security program.

3.1.1 Approach

Before requesting or acquiescing to deployment of public security forces, the company should perform a Job Safety and Security Analysis. This procedure reviews all the facts about an upcoming or proposed activity: its potential risks and the need, costs and benefits of mitigating them. An armed presence of

public security forces is justified if there is a serious risk to life. However, if the only way the activity is safely performed is with a public security force escort prepared to use lethal force, then the question must be asked, "What possible gain justifies the risk of proceeding?"

Decision Tree for Requesting Public Security Forces



Scenario 7: Artisanal Mine Confrontation

An incident occurred when a technical team entered a sensitive area to evaluate a site occupied by artisanal miners. An armed police officer accompanied the team. When a large group of artisanal miners became hostile and moved threateningly toward the team, the officer attempted to defend his life and the team by firing his weapon, which did not function properly. The police officer and the team members scattered and ran. Fortunately, no one was killed.

1. If the company did a JSSA, it apparently misinterpreted the available information and underestimated the risk prior to sending the team into the area.
2. Company security was not the first line of protection.
3. The officer was ineffective as a deterrent, did not know how to maintain order and failed to protect the team.
4. In a life-threatening situation, the policeman was unable to use his weapon effectively. The reasons for this are unknown to this author, but are irrelevant. If lethal force is required, it must function.
5. Command authority in an emergency was unclear. At some point, the policeman transitioned from escort to the authority in charge of using lethal force. It appears unlikely that all team members, including the policeman, understood this transition or discussed it prior to the event, so that each knew what to do in a crisis.

As the saying goes, hindsight is 20/20. In addition, numerous other factors influenced this event. Nonetheless, it was extraordinarily fortunate there were no serious injuries or fatalities.

For Discussion

How do the capacity and skill of the public security forces influence the company's ability to implement the VPSHR and what can be done to mitigate the risk?

Use Company Security First

The company's contract security force is the first line of protection for the lives, property, business continuity and reputation of the company. The company should never ask for a public security forces deployment in lieu of company security. Public security forces are the back-up if the company security cannot handle a problem. However, company security cannot perform the legitimate legal duties of the public security forces. Therefore, resort to the public security forces is an essential and legitimate component of any security program. To minimize this last resort, company guards should have a robust capability to handle problems.

Minimize Public Security Presence

There are four levels of public security presence:

1. *On call.* Local forces are located at their normally assigned location in the community to maintain law and order. Public security in this case is the least visible, but also the least responsive. To come to the company's assistance, they will need transportation to an incident, communication and reasonable availability, free from other commitments.
2. *On location, but out of sight.* Public security forces deployed to company facilities are more readily available, better aware of the conditions and vulnerable points at the location. They can train and exercise with company security to ensure the incident response procedure is coordinated. This will reduce the likelihood of misunderstandings. Company security guards will take comfort knowing help is close by. Keeping public security forces separate from the scene is usually the best way avoid a menacing presence. It allows the company the flexibility to escalate protection as a response to threats or a deteriorating situation. This presence incurs the cost of transporting and maintaining the public security forces (meals and accommodations) and may include other per-diem and call-out fees.
3. *On location, but visible and in reserve.* Bringing public security forces visibly to an incident location is a significant escalation of force. It can be useful to demonstrate resolve, deter violent behavior and calm passions. Bringing public security members on location can also inflame a situation. This should be a conscious decision by management, never done automatically. Once a public security officer is present, the company loses some control over the security operation. As long as they are in the background, the company's security representatives can retain tactical control of an incident. Once on scene, however, the commander may act unilaterally, especially if there has not been extensive coordination, preparation and rehearsals of incident response. This level incurs similar costs to those of Level 2.
4. *Deployed to respond.* Once public security forces are committed to help control an incident or situation, the company's control over events is compromised or lost. The public security forces may use deadly force if they perceive a need, regardless of what the company expects or requests. Bringing them to the point of confrontation should be a last resort to protect lives and re-establish order and control at imminent or actual violence. Management should carefully weigh the deterrent value of bringing public security forces into the situation against the possibility of excessive force or other unintended consequences. Therefore, it is the least desirable posture and should be the last resort.

Memorandum of Agreement

The potential need for public security forces justifies an agreement concerning the conditions, expectations, obligations and standards of behavior outlined for all parties.[1] The ideal outcome is a binding agreement that specifies the responsibilities and obligations of the company and the public security forces, signed by the senior leadership of the company and the respective agencies with detailed implementation instructions at subordinate levels.

---

1 The title and format of this agreement depends on the requirements of the parties. It may be a Joint Protocol, Memorandum of Agreement, Memorandum of Understanding or Letter. The content is more important.

3.2 SECURITY ARRANGEMENTS

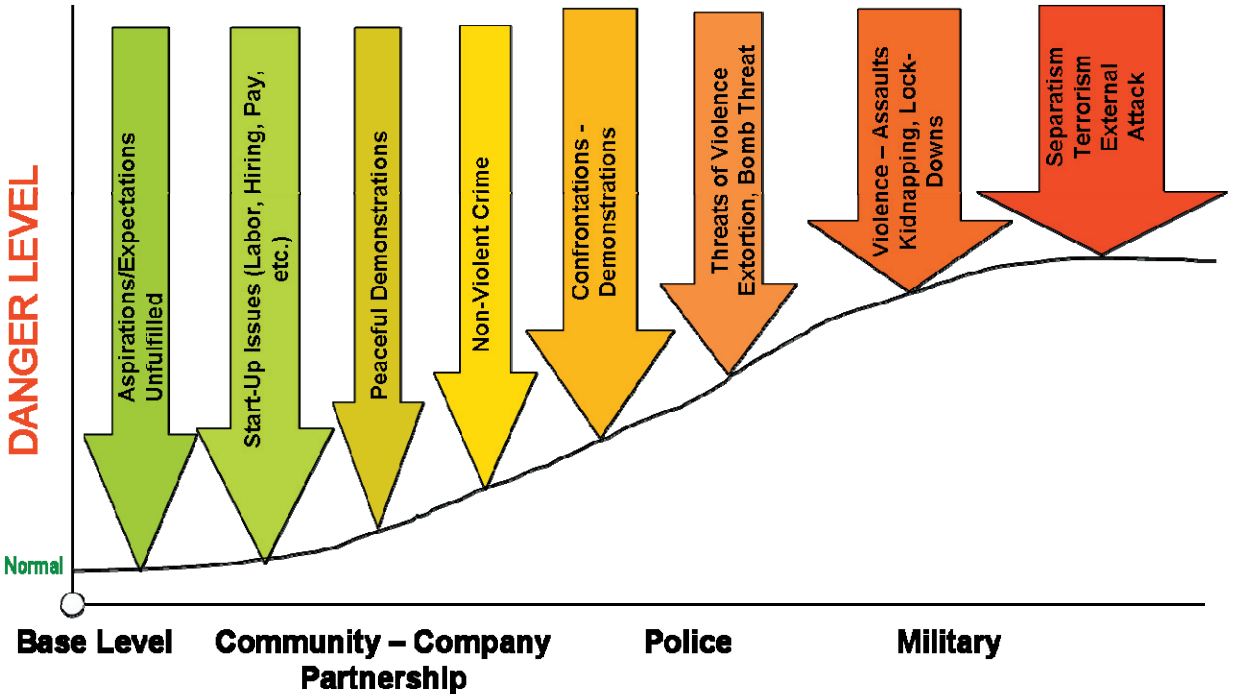
The VPSHR encourage private corporations to have consultations and other appropriate arrangements with the security forces of the host nation. With due regard for necessary confidentiality, these arrangements should be as transparent as possible. The company should take the initiative to sign a protocol agreement with the government (including at provincial level where relevant) concerning company support to the host government, including its security forces. This initiative will provide a bridge to develop supporting security arrangements and standard operating procedures (SOP) with the public security forces and other public security forces. These arrangements should include the VPSHR as a jointly agreed standard, if possible.

3.2.1 Discussion

Security arrangements are essential to protect the company across the full spectrum of security threats. As the diagram below illustrates, the public security forces have a responsibility to the people and the nation against all levels of violence. As the level of violence increases, from normal criminal activities through invasion and war, the nation's resources become more committed to the effort to re-establish and maintain peace, law and order.

Because the company may decide to continue operations across virtually the entire threat spectrum, it should be prepared to engage all relevant state agencies. Obviously, this is best done before a crisis, setting standards and clarifying expectations as fully as possible.

Security Continuum



In developing the company's approach to the public security forces, some guidelines that support the values of the VPSHR are helpful:

1. Any arrangement will be legal, ethical and moral.
2. It is appropriate to define mutually agreed standards of behavior and conduct.
3. Any agreement should have clear wording when describing obligations, expectations and commitments of the parties.
4. An openly signed document is better than an unsigned one; an unsigned "White Paper" is better than a verbal agreement; a verbal agreement is better than an implied understanding; and, any of these is better than no agreement or contract at all.
5. All agreements, even verbal ones, are subject to disclosure. Therefore, it is better to be as open and transparent as possible with the expectation that, eventually, the agreement will enter the public domain.

Once the company has negotiated and signed a protocol agreement with the regional or provincial government on support to the public sector, the company can begin coordinating the supporting agreements governing the deployment of the local police and, where this is appropriate, the military forces to the company's sites. The goal of any agreement with the police, military and other public security forces is to reduce ambiguity and establish accountability. The company's legal department and government relations manager will review all agreements with government institutions. The review is for conformity with company practices.

On occasion, the legal or social outreach managers may be reluctant to engage the public security forces in a formal agreement. Their concerns are important; however, the advantages of a clear agreement outweigh other concerns. *Ad hoc* arrangements cobbled together in a crisis never work as expected and frequently prove ineffective.

Key elements of a security agreement include:

- Company's adherence to the VPSHR (preferably the host nation's adherence as well);
- Provision for routine consultations, coordination and information sharing;
- Method(s) to request support by either side;
- Designated points of contact and coordination;

Achieving agreement with the public security forces, *beginning with the police,* then military forces and then other state security forces, can be delicate. In leading the discussion to develop an agreement, it is often helpful to use existing host nation laws and agreements. These usually include acceptance of the relevant United Nations conventions on the use of force, detention of persons, Universal Declaration of Human Rights, Convention Against the Use of Torture and similar international standards. The company should emphasize it is using these laws, treaties and agreements as references in its proposed joint agreement where this is appropriate.

It is highly desirable to ask the government authorities to accept the VPSHR as part of the agreement. In doing so, the company should make it clear that it has agreed to adhere to the VPSHR. The company may also note that other companies operating in the host country, and most major extractive industries worldwide, operate in conformity with the VPSHR process. Including the VPSHR as part of an agreement between the company and the host government demonstrates the government's commitment to internationally accepted norms of behavior.

In securing agreements with the military forces, it is sometimes advantageous to begin with the navy or air force as they are less directly involved and may be more comfortable operating according to international conventions and protocols.

The relationship with the national intelligence agencies is even more delicate. On occasion, the internal intelligence service assigns members to a company site to perform limited duties, usually for an early warning of potential trouble. Though uninvited, the intelligence agencies can be helpful in providing information about the wider region and province that can assist company's own information analysis. If domestic intelligence agencies assign their representative to the company's sites, especially if the company must, to some extent support them, then it is appropriate and responsible for the company to formalize this relationship in a protocol or MOU. Ideally, this will allow the company to get clarity on the missions, authority and limitations of its representative on site. The company should certainly request recognition and respect for the VPSHR. At the least, the protocol should include the process for reporting inappropriate behavior. It is reasonable to invite their representative to participate on a volunteer basis in the human rights, first aid, safety and other similar generic training. The more benign their presence, the better it is for all stakeholders.

3.2.2 Recommendations

1. Negotiate agreements with public security forces command at the local level that define their role in standard operational procedures (SOPs) and in extraordinary or emergency circumstances. This agreement should specify that it covers all company activity in the area.
2. Upon completion of the agreement with the police, review and make appropriate revisions for similar agreements with the military and national intelligence organizations if relevant.
3. Include the VPSHR as a reference for the documents along with the relevant host country laws that relate to the protection of individual and human rights. Attach the VPSHR as an appendix to the protocol agreements.
4. Explain this process at all levels of the public security forces and ensure that there is no appearance of impropriety. The company may need to conclude separate agreements or memorandum at both the national and local levels.
5. Keep other extractive industries informed. They should be able to add impetus and momentum to the process without inhibiting it.

Advantages

- The existence of established protocols for implementing procedures provides the company an invaluable structure for dealing with public security forces.
- Joint agreements reduce ambiguity and raise mutual confidence and respect among the parties.
- The agreements can establish the mechanism to introduce professional training activities.
- A comprehensive agreement should establish the criteria for introducing and, if necessary, maintaining police or other public security forces at company facilities.

Scenario 8: Promoting the VPSHR to Governments

Companies are often reluctant to jeopardize their relationship with governments upon which rests many commercially sensitive decisions. However, governments in the developing world are far keener to enhance their international standing than many companies suspect. Membership in a variety of international institutions, like the United Nations and World Bank requires or at least encourages demonstrable progress in respect to human rights.

Public adherence to the VPSHR supports the position that governments are responsible, accountable and respectable. In short, asking governments to accept the VPSHR may be akin to pushing on an open door. For example, in Colombia, Indonesia, Democratic Republic of Congo, Azerbaijan, Georgia and Turkey, companies have been successful in negotiating agreements with public security forces that commit all parties to follow the tenets of the VPSHR.

For Discussion

What are the opportunities for your company to promote the VPSHR in the countries where you operate?

- Formal agreements reduce the potential risk of human rights abuse and inappropriate use of force.
- In addition, they demonstrates the way forward for other companies to adopt the practice.

Implementation Risks and Mitigation

- Negotiations can be time-consuming. The company will have to consult with multiple levels of the host country government and convince them of the usefulness of this initiative. The company will have experience, however, in successfully negotiating business agreements and other protocols and agreements. This process is procedurally similar.
- An agreement does formalize the company's relationship with the host country government in an area that is beyond normal commercial activities. Protocols and similar agreements are standard in the extractive industry and good business practice.
- Like other legal processes and contractual agreements, this will require a dedicated effort to clarify commitments and to keep expectations in check. This report provides examples of language that may assist in drafting an agreement. A workshop with an internationally respected legal expert may help further.

3.3 DEPLOYMENT AND CONDUCT

At first glance, the company's managers may not believe they have much control over the deployment and conduct of public security forces. Nevertheless, the company can use its presence, and any in-kind support it provides, to shape the deployment and conduct of state security forces.

3.3.1 Relevance to the VPSHR

Studies of human rights abuses in conflict areas repeatedly identify the main causes of such incidents as (1) weak, ineffective leadership, (2) lack of discipline, and (3) improper equipment. The dangers of the first and second of these causes can be reduced by taking care in managing the deployment of public security forces. It is essential when public security forces deploy that all concerned know the ground rules. These forces must be able to perform the legal duties, but still maintain the appropriate standards of behavior and protect the rights of those involved.

3.3.2 Overview

The host country normally has limited security resources and many requirements. The government may elect not to direct the deployment of public security forces to a company's facilities if there is no imminent threat or request from the company. In other cases, the host government has directed the deployment of forces to the company's facilities. That has happened in the past with some companies, and on at least one occasion the demands of an army commander for support eventually involved one company in a lengthy court case. Thus, there is a demonstrated need for a protocol governing interaction between the company and the government that addresses the issues of public security forces deployment.

The company's challenge in hosting public security forces at its sites and facilities is to make sure that it does so in a way that serves the best interests of the company, the community and the state. To do so, the presence of public security forces must be necessary; they should behave appropriately and handle any incidents transparently and in accordance with the provisions of law – in short, consistent with the VPSHR.

3.3.3 Discussion

Deployment of public security forces to the work site inherently brings the possibility of unwanted or inappropriate behavior. It publicly identifies the company with the presence of police or military in a location and at a level that would not otherwise be the case. Whatever the police or soldiers do, this will inevitably reflect on the reputation of the company. Therefore, the company should only request

such a deployment because of imminent threat or after an assessment that the company cannot manage a potential threat without public security forces on site. This could be because there is a high level of lawlessness, or because the site is so remote that the response time for public security forces to arrive exceeds the ability of the company's private security forces to manage security risks and protect the site.

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. Therefore, the company should take whatever steps possible to ensure their behavior meets acceptable standards. The public security forces should understand their role and responsibilities and be under positive control by their chain of command at all times. The procedures for involving the public security forces in an incident should be clear to company management, the security department and the public security forces themselves. The company and public security forces should agree and specify procedures for the use of lethal force in the rules of engagement (ROE) as part of any agreement to bring them to the site. As soon as possible, the public security forces assigned to the company's facilities should receive instructions concerning the VPSHR and International Humanitarian Law.[2] The security forces will also require written SOPs and guidance concerning their behavior. A detailed briefing by their commander, instruct-ing them in the standards of performance of their duties is essential. This course of action is equally appropriate if the public security forces unilaterally decide to deploy to the site and demand support.

Local public security force commanders are often receptive to working with the company to establish mutually agreed Rules of Engagement for the use of force. These rules then should become a part of any training the public security forces do prior to deployment to the company's facilities.

The company should also designate any public security forces assigned to their facilities as the Security Emergency Reserve, held in readiness as a response force and not routinely used for guard duties. The authorization to commit the public security forces from their reserve position to take action at an incident site should be limited to the senior company manager at site, exercised through the site security manager. Their criteria for committing the public security forces should normally be:

- A felony has been committed requiring a policeman or magistrate to investigate and make an arrest.[3]
- No other course of action is likely to be able to protect life and limb.

By most standards, the public security forces at site are a *de facto* arm of the company's security department. The community will lay any indiscipline, criminal acts or human rights abuse committed by the public security forces at the door of the company, as will international NGOs. The company should therefore take prudent steps to perform background checks and maintain records documenting the public security forces assigned to the site[4]. Using the techniques recommended in 2.4, Human Rights Records, document all public security personnel assigned to the site if possible.[5] At the minimum, the company should perform background checks on those in supervisory and command positions for past criminal behavior or human-rights abuse. Check this list of names against any known credible allegations or reports. These same circumstances apply to the state intelligence personnel present at site.[6]

---

2 Ideally, the International Committee of the Red Cross (ICRC) can provide the humanitarian law training; it is mandated to conduct such training and is accredited in most countries in the world.

3 In some countries, a specially trained official, who is usually but not always a policeman, has the exclusive power to investigate a crime and prefer charges. In such countries, the police or a private security officer may make a detention until the official can arrive and conduct his inquiry.

4 This would be useful in refuting allegations that the company permitted known human-rights abusers at the site and documenting who was present at what times.

5 In some cases, for example, when hundreds of soldiers or police are rotating through a site on a frequent basis, it may simply be impossible to check them all and maintain the necessary records.

Regardless of the location, the public security forces will have a responsibility for maintaining law and order and responding to serious incidents. The best way to ensure the public security forces, company security and local site mine management have mutual confidence is through a thorough preparation for possible contingencies. This means joint drills and rehearsals for incident management. Rehearsals are relatively easy to conduct and should address the phases of an incident response including:

- Preparation and review of Rules of Engagement,
- Alert,
- Deployment,
- Designation of the on-site team leader,
- Actions on contact,
- Resolution of the incident,
- Provision of medical attention if required,
- Review of post-incident lessons learned,
- Final reporting and follow-up.

An excellent method of rehearsals is to use the "talk-through, walk-through, run-through" formula. The purpose of such rehearsals is to communicate all tasks and expectations, including limitations on the use of force, to all participants (public security forces-mine security-management). The second step is a walk-through with a discussion at each step of the actions and responsibilities of the participants. The 'graduation exercise' is a full-speed run-through with role-players to simulate the perpetrators. These training events are most effective if the scenario for the simulated incident is plausible or even a repeat of a previous incident. The main objective is to reduce confusion, make sure all concerned know what their duties are, reduce ambiguity and uncertainty and build mutual confidence and trust among the participants. Like any actual incident, the company should fully document these rehearsals.[7]

As these steps proceed, the company can strengthen its overall safety and security by fully explaining the developments to the other security stakeholders. The company's employees will experience the impact of changes in the presence and posture of the public security forces and could become alarmed if they misinterpret what they see. Because the local communities are directly affected by the presence or absence of public security forces in the local site area, these communities should be informed and consulted as part of the process. Local government and the other security services may undertake adjustments in their own operations as a result.

3.3.4 Recommendations

1. Review the Threat Register and Risk Assessment to determine if the threat justifies a public security forces presence at the site. Identify alternative deployment options and methods of response.
2. Work with the local public security forces commander to draft appropriate Rules of Engagement consistent with UN standards and the VPSHR.[8]
3. Consolidate all public security forces at site in a central location and designate them the reserve force for emergencies only. Ensure they have adequate transportation to respond rapidly to an incident location.

---

6 The presence of the state security forces assigned to the site may be beyond the company's control. At the earliest opportunity, however, the redeployment of this presence should be requested. The company cannot sustain a case for the need to have the state security forces present if it is only for the protection of the mine.

7 There are number of international firms that specialize in providing such training. On balance, the company is the better manager of this effort, rather than delegating it to the guard service contractor.

8 Once the ROE are promulgated, the company should have these printed as handout cards and given to each public security forces member assigned in the company's site area. This could be encouraged by engaging with the provincial public security forces commander to gain his support and approval.

4. Identify the persons authorized to deploy the public security forces from reserve status to incident response. This responsibility should be limited to the site manager and the security manager, or their alternates if they are not present and specified in the agreement with the public security forces.
5. Establish a scenario-based set of rehearsals and incident management drills involving all participants who will perform duties in a real event.
6. Communicate the developments through the Community Security Forum, described in Section V.

Advantages

- Reducing or eliminating the public security forces at site reduces the possibility of an incident caused by accident or indiscipline.
- Establishing ROE gives each individual public security forces member and supervisor clear document lines and reduces the chances of excessive use of force.
- Public security forces in reserve allow better command and control of the public security forces, reduce the intimidation factor and limit premature undesired involvement.
- A clear hierarchy defining those in charge and having authority to direct action reinforces centralized control of an incident.
- Additional training and rehearsal increases the probability that all concerned will act appropriately, under firm control and in accordance with expected norms of proper behavior.

Implementation Risks and Mitigation

- Redeployment of the public security forces may diminish the deterrent effect of a visible presence and encourage criminal or confrontational actions. Periodic joint company/public security forces patrols will continue to demonstrate the public security forces remain available to address their law enforcement role.
- Close coordination with the public security forces on ROE, scenario-based training and joint rehearsals is time and resource intensive. An external training consultant or company is an effective and efficient way to develop the training program and materials to the company's specifications and international standards.
- Drills and rehearsal may alarm those who are unaware of what is happening and why. Public announcements and notifications will manage this concern.

Resources

The resource implications of redeploying public security forces are minor and may even reduce the over all costs by reducing 'in kind' support to the public security forces at the company's site(s). The security manager can take the initiative to assist the public security forces in developing Rules of Engagement.

3.4 CONSULTATION AND ADVICE

3.4.1 Relevance to the VPSHR

Consultations and advice between companies and the full spectrum of public security forces are a useful conduit to promote respect for human rights and proper behavior of the security services. A strategy of engagement is important if the consultations are to progress beyond casual discussions at the local level. As part of the engagement strategy, the company should recognize the value of a modest investment in training and education on international standards of behavior for the public security organizations. This applies particularly to the police, and to the military as well where they have a direct role in providing security to the company.

3.4.2 Overview

A basic tool in managing the company's relations with the public security forces is close, regular communication and consultation. Companies often have a good track record of meeting with the authorities in their local site area. At the local site the security manager and deputy may interact daily with the public security forces. The main thrust of these meetings is routine coordination of the public security forces presence at local site (if there are public security forces assigned), exchange of information concerning possible risks in the region and other technical matters.

There are opportunities for furthering the local security forces' understanding of the VPSHR and enhancing their awareness of human rights standards. A strategy to engage the police and other public security forces will be useful in focusing effort and identifying specific measures for each of the public security counterparts. This strategy is integral to and in alignment with the overall program of stakeholder consultations.

3.4.3 Approach

The company's engagement strategy with the public security forces should include these goals:

1. Maintain and enhance the regular scheduled meetings between all relevant the public security forces and the company.
2. Engage each echelon of public security forces command, develop a relationship with that commander and agree to maintain contact and share information (i.e., a no-surprises policy).
3. Negotiate and sign a site security document that supports the overall company/public security forces protocol and clearly outlines the specific responsibilities, expectations and standards of each party in maintaining security for the company at the local site.[9]
4. An effective engagement strategy addresses each echelon of the host nation's national public security forces**.**

Relations with the Local Public Security Forces

Periodic meetings between the public security forces and the company security professionals are critical to establishing and maintaining safe and secure operations. Local site meetings are usually informal and should remain an opportunity for the participants to discuss potential security problems and determine appropriate responses. The company can strengthen this relationship by inviting the public security forces command in the area to participate in occasional social events such as a soccer match with company employees, etc. This promotes mutual understanding, builds confidence and "humanizes" each party to the other. Within the boundaries of the relevant home country legal limitations, the company should seek opportunities to work together with the public security forces in joint projects for the betterment of the community. For example, an assistance project to benefit a local community, undertaken jointly by the company and public security forces, followed by an appropriate ceremony and social event, could be a win-win for all concerned. The objective is to make the local unit a showpiece for the national public security forces in how to manage a professional relationship.

Regional or Provincial Level Contact with the Public Security Forces

In countries with a regional structure, It is imperative that the company security manager meet with the regional public security forces commander(s) at the provincial public security forces headquarters on a periodic basis. Again, within the relevant legal and corporate policy guidelines, the company's senior local representative and the company's senior country manager should host regular contact events with the provincial public security forces authorities, preferably not less than quarterly. It is important that the public security forces see company's commitment to open communications. These

9 This site-specific agreement would not encompass other company activities and operations as their special circumstances would require an agreement specific to each local situation.

events will also allow management to update the security commanders on an informal basis about the company's operations and activities. The security management team should definitely attend these events, and where appropriate identify local developments that may have a security impact. The formal meetings and informal social events are occasions to discuss issues that cannot be resolved at the local level. The goal is to keep the local public security forces commanders well informed about the company's activities and confident that the company is working with them in a spirit of transparency and cooperation. Unless there is a real emergency, all issues should be discussed with the regional security commander before taking them up the chain of command.

At the national level, the company will no doubt have representation at the capital. The company's senior representative there is the appropriate responsible party for establishing and maintaining a close relationship with the senior state security authorities, especially the police and Interior Ministry. Most policy issues are decided at the capital. The company security manager or deputy manager should participate in these periodic discussions with the national public security forces commanders whenever possible, at least annually. National public security forces, especially police, are usually most interested in developments that may affect their operations, require redeployment of scarce resources and threaten national cohesion. They are also normally concerned about the proper deportment of their subordinates. The company's security manager should be aware of any issue that could affect these concerns. In turn, he can solicit information from the public security forces that will alert company management to any pending actions or security concerns that could affect the company's operation. Again, consistent with corporate policies and legal constraints, the security manager should look for opportunities to engage the public security forces in activities that build a relationship of trust and mutual confidence at the senior level. One effective method to strengthen that relationship is to sponsor a visit by senior public security officials to the company's operational site. The effect on their chain of command is normally very positive and enhances the position of the company with local commanders. These steps strengthen the company management's access in difficult times. The company representative can pick up a phone and ask for help at a senior level to resolve problems with local commanders. This access is also a powerful potential deterrent to subordinates who may be tempted to step over the line and abuse their authority.

3.4.4 Capacity building

A number of initiatives can promote proper standards and enhance professionalism in the host nation's public security forces. This effort is extremely important for the long-term welfare of the inhabitants of the company's operational area and the company's own security. As the company interacts with the national public security forces, it is important to remember that they have probably not had access to the proper resources, training or equipment necessary to reach the standards they would like to achieve. In most developing countries, the public security forces are under pressure to reform and achieve a higher standard of professionalism and efficiency. The company has an opportunity to work with the public security forces to raise their professional standards in ways compatible with host nation laws and accepted standards on international business practices. This is consistent with the VPSHR. Indeed, an educational briefing on the VPSHR should be part of all agreements with the local and national public security forces. The objective of this effort to build professional capacity is to make an assignment to the company's operational areas a "plum" for the best and brightest of the national public security forces, a place where public security forces officers can build their careers through the opportunity to participate in advanced professional training and education programs. The guiding principles in developing cooperative programs with the public security forces are clarity of expectations and full transparency.

As a first step, the company should present an induction briefing on the VPSHR to all police and other state security forces' members assigned to the company's site(s). The company should also insist that all public security forces in the company's area of operations receive training in international humanitarian

law from the International Committee of the Red Cross (ICRC). The ICRC has a presence in most host countries; its International Humanitarian Law (IHL) program has trained thousands of public security forces and military personnel assigned to conflict areas throughout developing countries.[10] The company should request the public security forces to certify, by name, that any assigned and all incoming public security forces have received this training as part of the support agreement between the company and the public security forces. To meet this standard it may be necessary for the company to resource the travel and *per diem* costs for public security forces trainees to attend the training sites, especially if there are no courses in the local area or province. Additional training on subjects such as the UN Code of Conduct for Law Enforcement Officials, Principles on the Use of Force and Firearms, should be a part of the minimum standards for assignment to the company's operational site(s). In all likelihood, the company will have to offset the costs of this training. The UN Mission, if there is one in the host country, may also have conducted public security forces training programs reaching hundreds of individual public security forces members. It may be able to address some of these training requirements. The European Union, Japan and several other bilateral donors also have public security forces training and professionalism programs that may be helpful. Finally, a number of private companies offer internationally recognized public security forces training programs complete with certified trainers. The more training public security forces receive the more likely they are to improve their professionalism and proficiency and thus the brighter their promotion prospects. The company should carefully monitor such training to assess its impact.

3.4.5 Accountability

Accountability is the most important factor in establishing and maintaining discipline in any organization. The host nation's public security forces are no exception. Recognition of proper performance and professional conduct is an important part of encouraging appropriate behavior. Identifying breakdowns in discipline will likewise direct the attention of commanders to those personnel and procedures requiring corrective action. To support and reinforce these standards, company security should prepare a monthly Security Status Report that summarizes all significant security incidents and developments and the actions taken during the reporting period. The on-site police commander (if there is one), the local police chief and the provincial chief of police should all be on distribution for the report. Serious

Scenario 9. Police Training

A corporate project in a very remote location wanted to assist the police in building supervisory capacity at the local level near the site of their operations. Fortunately, a respected international police training program was about to conduct professional enhancement training in the provincial capital several hundred kilometers away.

Unfortunately, the police did not have the training budget to support travel and accommodations for those outside the provincial capital city. After coordinating with all concerned, the project funded the local and district level police commanders, four persons, to attend the two-week course. The police chiefs received training otherwise not available to them, the provincial police were pleased that front-line police were able to participate without additional cost to their limited budget and the international trainers were enthusiastic about adjusting their course load to include four more students.

The costs were nominal to the project, but demonstrated their commitment to help improve the capabilities of local police supervisors, enhance their competitiveness against their peers and strengthen mutual respect. The local police got something of benefit to them and the community that was completely transparent and appropriate.

For Discussion

What opportunities exist? What risks and mitigation exist?

10 The ICRC also educates civilians about the rights under IHL. For a full description of recent ICRC efforts concerning International Humanitarian Law training see their respective country websites at *www.ICRC.org.*

infractions, with any corrective action taken, should be a part of this report. At each level, the police chain of command is accountable to their higher commander, both for the successes and shortcomings of their command. They will have the opportunity to show they have taken prompt action when required. When the police handle an incident or request with exceptional professionalism, the company should forward special commendations, included in the report, and letters of recognition through the police chain of command to those deserving recognition. It is appropriate to include a nominal gift such as a T-shirt, ball cap, ballpoint pen or Frisbee with the laudatory letters.[11] The value of any such item should be less than $25 and registered with the company's legal and ethics department to preclude charges of impropriety.

3.4.6 The Host Country's Military Forces

The military forces of the host country have a sovereign requirement for planning and conducting national defense and for reinforcing the police when requested. In situations where the police lack the capability to maintain order, the military forces have the duty to be ready to respond. Therefore, the company should engage and consult with the military forces in ways appropriate to their national defense role.

The company cannot ignore the military forces, but may adjust the relationship depending on national developments and the evolving role of the military forces. Company representatives should maintain close contact with the military forces representatives at each command echelon, though this may not be as frequent as contacts with the police. The military headquarters at each command echelon has important responsibilities and will have key points of contact and liaison; the company should not overlook or ignore these important headquarters. Doing so will invite complications and risk inappropriate activities by units who assume they are out of the spotlight of accountability.

As with the police, the company should request that the military forces ensure all local military units assigned to the site area receive regular ICRC-conducted IHL training if this is available.. The ICRC program often achieves its best success in training with the army, so this initiative should not provoke a negative reaction from military authorities. If the company takes the initiative to arrange for training in UN standards and principles for the police, it should extend invitations to join courses by the internationally recognized human rights subject-matter experts to the military forces as well.

3.4.7 Recommendations

1. Develop an integrated engagement strategy for the company's interaction with the host nation's public security forces. This strategy should address each echelon from the site to the national capital inclusive.
2. Establish standards and set expectations that local public security forces, especially the police and military forces, will accept. Encourage their participation in ICRC conducted IHL training.
3. Engage with an internationally respected training and assistance organization to conduct essential, non-lethal, professional training of public security forces, if necessary. Explore international donors for synergy in supporting public security forces reform and training programs.
4. Ensure this process is briefed to all levels of the public security forces (police, military forces and intelligence agencies) so there is no appearance of impropriety. A separate agreement or memorandum at each level from national through provincial to local is usually appropriate.
5. Keep other extractive industries informed. In many cases, they will also add impetus and momentum to the process without inhibiting it.

---

11 Representational items with the company logo and a security related message will further reinforce good behavior.

Advantages

- The existence of an established protocol with implementing procedures provides the company an invaluable structure for dealing with public security forces.
- A joint agreement reduces ambiguity and raises mutual confidence and respect among the parties.
- The agreement can establish the mechanism to introduce professional training activities.
- An agreement establishes the criteria for introducing and, if necessary, maintaining police or other public security forces on to company facilities.
- A formally agreed procedure reduces the potential for human rights abuse and inappropriate use of force.
- Such an agreement provides an example for other companies to adopt the practice.

Implementation Risks and Mitigation

- Negotiations can be time-consuming, as company management will need to consult with multiple levels of the host country government and convince them of the usefulness of this initiative. This suggests early commencement of the process and can be included as part of any protocol(s) already under negotiation.
- An agreement formalizes the company's relationship with the host country government in an area that is beyond normal commercial activities. Working with responsible NGOs on this issue will reduce the risk of criticism.
- An effective agreement demands a diligent effort by all parties to clarify commitments, maintain transparency and keep expectations in check. The best way to manage these expectations is by clear discussions and transparency. The monthly Security Report to the public security forces chain of command is also a way to be specific about what is offered and underway.

Resources

The company management at each level, local through corporate, will be involved in the discussions with host nation authorities at the appropriate echelon. Management cannot delegate this issue to the security managers if the program is to have real credibility with the local authorities. At provincial and national levels, management may include the VPSHR as a talking point in wider discussions. At the local and site levels, company management should dedicate the time to make the VPSHR the topic for a separate meeting.

International donors may have existing programs to provide professional training in professional conduct and human rights to host nation security forces. The ICRC has separate funding and cannot accept direct support for its International Humanitarian Law training. In both cases, however, the company may serve its own interests by supporting travel and *per diem* costs for isolated public security forces officials. The costs for this are usually low and depend on a number of factors, including numbers of personnel and travel costs.

The company may have to provide some critically important training on human rights, UN Standards on the Use of Force, etc. This is a recurring cost because security services usually rotate their personnel periodically, so both initial and sustainment training are a continuing requirement.

3.5 HUMAN RIGHTS ABUSE

3.5.1 Relevance to the VPSHR

Of all the components of the VPSHR, reporting human rights abuses is the more specific and contentious. Unless there are clear and effective methods for taking action when credible information comes in, the company may flounder at the critical time. Failure to take action can be interpreted as complicity in the abuse.

3.5.2 Overview

Allegations of human rights abuse are always serious and demand immediate attention. The expectations in dealing with human rights abuse as outlined in the VPSHR are clear. The company should have a simple and effective plan to monitor the local area of its operations, gather and record information if an allegation surfaces and then document the response. If the allegation appears substantive, the company will report the incident to the proper authorities and request a thorough investigation and appropriate disciplinary action if the facts warrant.

The company should prepare for this situation by establishing a process, explaining it clearly in advance to all security stakeholders, particularly its employees, the local community and the state authorities. Confidentiality is an essential component of the process to protect the victims, witnesses, and others involved. Confidentiality, however, is not an excuse for failing to maintain complete records.

3.5.3 Discussion

The company's corporate reputation is a valuable, if intangible, asset. Several large corporations have suffered considerable damage and become the favorite targets of activist NGOs, because the corporations failed to operate as a good citizen and neighbor when they could and should have. The VPSHR oblige signatories to take reasonable measures, which include:

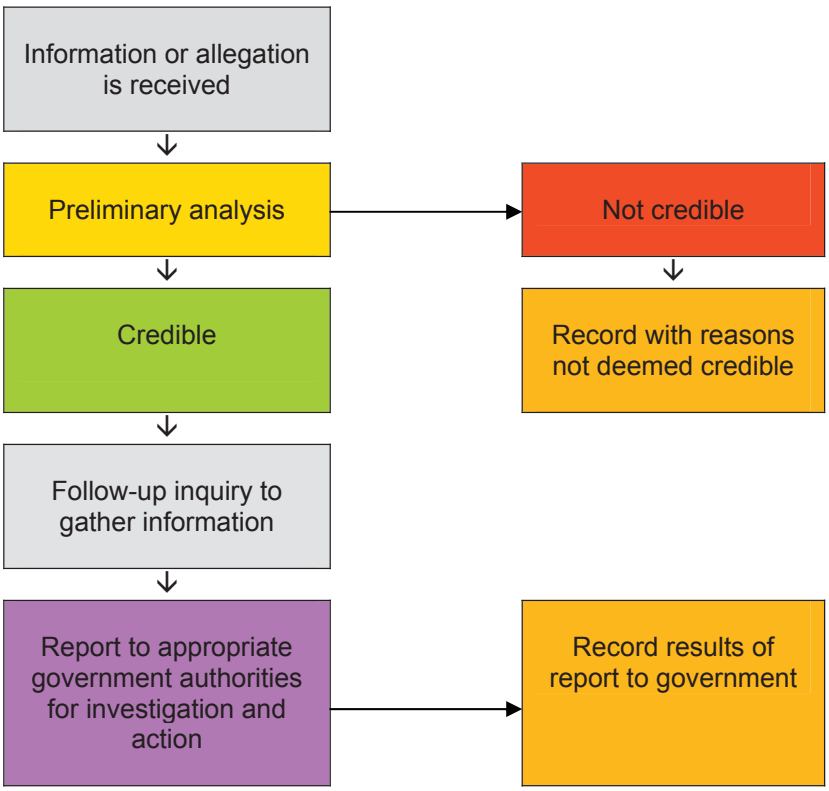
- recording and reporting allegations,
- monitoring investigations and pressing authorities for results,
- monitoring company provided equipment,
- trying to verify the credibility of allegations, protecting sources and sharing subsequent information with those concerned with the investigation and follow-up.

Allegations may reach the company from a number of sources. The two most likely conduits are from the social investment staff members who work in the local communities daily. They may hear rumors or possibly see evidence of a human rights abuse. Company management should insist that employees report any suspicions through their immediate supervisors to management. A second source of information is the contract guard force. Many of the members will be local residents and exposed to the general flow of information in the community. In both cases, there may be reluctance to report a suspicious incident. Perpetrators of human rights abuse count on fear of retribution or the expectation of protection by their superiors to act with impunity. Company staff must be educated about the obligation to report allegations so that appropriate inquiries can take place. The company should make every effort to assure its employees that the company management will handle any allegations in a way that will protect those reporting the allegations from retaliation, but still bring the forces of justice to bear.

The company can receive confidential, anonymous reports of human rights allegations in numerous ways. These include a Report Abuse hotline, a computer address in the company offices that is solely accessible by a trusted monitor and a secure mailing address. Unfortunately, these methods are marginally effective where the work force has little access to telephones, computers or a reliable mail system. One possible way to facilitate gathering information is to use "tip boxes" located in areas where the work force has unobserved access to the boxes and can drop in anonymous notes, tips or other information. If authorities question the source of the original information, the company can state the information came from the tip box.[12] A tip box is not a common practice in developing countries. Managers will need to explain the purpose and procedures to the work force and community. The

12 The tip box is a way employees can report fraud, theft or other criminal behavior without putting themselves at risk.

Procedure for Managing a Human Rights Allegation



value of the tip box is not exclusively the number of useful leads that result. It is also the fact that the company has provided a method to permit sensitive information to reach management.

If an allegation of a human rights abuse comes to the attention of management, the company should address the allegation through a serious and consistent procedure. The first step is to call the Site Security Committee[13] together to conduct a preliminary assessment. This assessment is to determine if the allegation is sufficiently credible to warrant further action. If the allegation is not credible, the Security Committee documents the decision in a memorandum for the record and no further action is required.

If the allegation seems credible, the Security Committee members begin a thorough analysis. Both security and social investment should use their information-gathering resources to verify the allegation. If the alleged incident occurred on company property, if it involved company equipment, or if it occurred

13 At this stage, only the site manager, security manager and social investment manager should be involved.

because of company activities or operations, then a full-scale internal investigation is required. A similar inquiry is appropriate for allegations that occur in the company's "areas of operations", a term not defined in the VPSHR. Obviously, there should be some generally acceptable geographic limit to what the company considers its area of operations. Beyond this area, the Security Committee should use its best judgment to determine if further inquiry is feasible and called for. The company is not a human rights NGO nor does it have trained human rights investigators on the staff. In gathering information about the allegation(s), the company has a simple objective to determine:

- Is it likely that something happened that warrants official investigation?
- Is it likely that the alleged incident involved the public security forces?

If the answer to these questions is yes, company management will refer the allegation to "appropriate host government authorities". This begs the questions of to whom to report, at what level and how. It is at this point that the company can draw on its efforts to build confidence and respect at each level of government, from the detachment sergeant of the public security forces to the ministerial level. The company will have informed the state security authorities at each level of the company's obligations under the VPSHR to take action when there are such allegations. The initial report of an incident, and request for investigation, should go to the lowest level that has the authority to conduct an incident

Scenario 10. One Method to Handle an Allegation of Human Rights Abuse

An allegation of a serious human rights abuse came to the attention of a security manager at a remote site. The abuse occurred some distance from the site, but within the same local police jurisdiction. A vague newspaper report seemed to confirm that *something* had happened in the area, but exactly what had occurred was unclear. The workforce, especially the guard force, was very concerned that local police were losing their discipline and accountability. Rumors flew and grew. Using the news account as the basis, the security manager (after discussing the action with project management) approached the senior police commanders supervising the local police chief. The security manager explained his obligations under company policies to follow up such reports and asked that the authorities investigate such an incident and take appropriate action, if any was justified. He also asked the police commander to release the results of the investigation in order to dampen community apprehensions. The security manager also privately informed an international NGO representative in the province of the alleged incident and asked that they follow up. The NGO would not provide feedback information, but they used their office to investigate allegations and ensure the public security authorities treat these seriously.

These actions were in accord with the expectations of the VPSHR, fulfilled the obligations implicit under the VPSHR and were effective. The senior police commanders were fully aware of the situation and did not become defensive because they were involved from the start. Using the news account as the basis of the request allowed the security manager to avoid naming his own guards and workers as the source of the allegations. This provided them with anonymity and protected the security manager from accusations of being a troublemaker.

The subsequent investigation resulted in the suspension and removal of the local deputy chief of police who had been the senior officer at the scene of the allegation.

For Discussion

How do you reconcile responsibility under the VPSHR and protect the relationship with public security forces? What ways could you approach the public security forces in your host country to report and follow up on allegations of human rights abuse?

investigation as long as that level is not itself implicated in the incident or any effort to cover it up. Usually, that is two levels above the likely perpetrators. For example, allegations that occur in the local area of operations are reported to the provincial commander of the implicated unit or individual.

Because each echelon of the public security forces and military knows that the company meets regularly with the next higher commander above them, the investigating echelon is more likely not to ignore a request for a thorough investigation and response.

In addition to reporting allegations to the public security forces, the company should also keep the provincial governor informed of its concerns. The company management should exercise discretion in this communication to maintain a cooperative relationship with the investigating authorities.

In most cases, it is also useful to pass the information and concerns to the ICRC for their action. The ICRC has a mandate to perform investigations of such allegations. The ICRC program has a well-established process for following up on such reports. They will maintain full confidentiality as to the source of the report. However, they will not provide any information concerning the results of their inquiry to a private person or organization, not even the person who reported the allegation. In many countries, there is also an official ombudservice or human rights agency with the responsibility for investigating human rights allegations. In some areas the Catholic Church sponsors church groups that do similar human rights investigative work. These multiple actors tend to encourage the appropriate authorities to perform a proper investigation and take disciplinary legal action where justified.

Lastly, the company should maintain its own confidential records of the events and actions taken. These validate that the company is fully meeting its commitments as a signatory of the VPSHR.

3.5.4 Recommendations

1. Create a formal Human Rights Allegations (HRA) Procedure that identifies points of accountability for each element of the procedure. Keep records of its implementation.
2. Make the Human Rights Allegations Procedure an open document. Explain it to the host country authorities at each echelon and to all security stakeholders. Post on the company website.
3. Establish tip boxes at locations around the mine site where information can be deposited anonymously.
4. Make contact with the ICRC delegate's office.
5. Make contact with the host government's agency that is responsible for independent investigation of human rights allegations, if one exists.

Advantages

- The HRA Procedure guides management in the proper and effective handling of a human rights allegation.
- The procedure explains to employees and others what to do if they hear of a human rights allegation and gives them a channel to report incidents.
- The tip boxes can also be a way for employees to report other criminal and ethical violations anonymously without risking retaliation or threats to their jobs.

Implementation Risks and Mitigation

- Responding to allegations is always delicate and can be mishandled, damaging the credibility of the company and embarrassing the organization. If the host authorities see consistency, respect, transparency and fairness in how the company responds to human rights allegations, they will be prepared and not be taken by surprise, and they will be more willing to work with this and other companies in the future. Company management should make this part of the normal discussions with all levels of the host country government (see Section VI below).

- Even in the developed world, first-line managers must explain the tip boxes and demonstrate to employees that suggestions and tips submitted to the boxes are valued and acted upon.[14] The company's objectives are best met by putting the tip boxes in common-use areas with clear instructions posted above them for all to read and understand.
- Company employees should be careful when conducting inquiries or gathering facts so they are not compromised or implicated in the incident.

Resources

- Publishing the Human Rights Allegations (HRA) Procedure and posting on the company website will have little additional costs.
- The costs of tip boxes, a telephonic tips hotline, a computer address and monitoring these will have minor budget and manpower implications.
- Training the managers, coaching the procedures, and conducting a workshop on the procedures should be a part of the overall VPSHR Implementation Program.

14 The TIPS hotline program in American cities annually solves hundreds of felonies. The lack of telephones and other communications equipment like computers makes the tip box the most viable option.

Relations with Private Security

In many respects, implementation of the VPSHR principles for company relations with its private security provider(s) is the most easily managed component. The company can specify standards for performance, mandate training programs, require reporting and certification, conduct audits and performance evaluations and hold the contractor responsible for the actions of its employees. (This approach holds also where security guards are hired by an EPC contractor, where the relevant requirements must also be included in that contract.) In addition, the private security company has much to gain by making the VPSHR part of their business plan. Doing so will confer a market advantage over competitors that do not use the VPSHR as a guide.

The company's challenges with private security are threefold:

1. Define the company's standards and expectations clearly, so that the private security company understands its performance objectives and deliverables.
2. Verify the successful delivery of these performance goals through an active and aggressive inspection, review and audit program of the contract security providers.
3. Communicate the performance standards to the other security stakeholders.

The company should clearly define contract performance deliverables with regard to the VPSHR. A company's security department often focuses the scope of work on guard coverage, equipment and supervision. Guard service companies, like all commercial ventures, are profit-oriented. They will tender for a service contract based on the scope of work as defined in the Invitation to Tender (ITT). Guard service companies calculate their bids on what will be necessary to meet the conditions set in that ITT, not on what is prudent or may be required to perform the job. Once the company awards the contract, however, the contractor is unconstrained by competitive pricing and will calculate accordingly. For that reason, the delivery expectations should be as detailed, clear and complete as possible. This will make for a better contract, fewer changes and a more successful and satisfactory performance.

Even the best contract is subject to problems if left unsupervised. In some cases, extraneous distractions enmesh a company's security staff, preventing them from frequent and thorough verification of contract performance standards.[1] In fairness to the guard service contractor, the company should use checklists and performance standards shared with the contractor, not later than the time the contract is awarded (preferably these should be in the ITT). At least monthly, the company's security department should send a performance report to the contractor's performance manager and the company's management.

The guard service provider is a component of the company's security department. Therefore, it is appropriate for the company to inform the other stakeholders of the security guard's required standards of conduct. As a minimum, this information sharing should include local hiring guidelines, prohibitions on the use of deadly force, and procedures for requesting police back-up. It is important to inform fully the stakeholders about the security program, but without compromising the security guards' safety or ability to perform their duties. Local communities in particular should understand their rights and responsibilities when dealing with company guards. The Code of Conduct and Rules of Engagement for the guards are not restricted information.

---

1 Security managers should judge their workload carefully. The security manager has an obligation to discuss their workload with company management if they become so over-burdened with peripheral duties that their main responsibilities suffer. The priority should always be on supervising the security program, including the guard service contract.

4.1 SETTING THE STANDARDS

4.1.1 Relevance to the VPSHR

The company can manage the contractual agreement with its private security provider to set standards of performance, particularly in the field of human rights. But, this requires active and focused management. It cannot be assumed as a given. A quality security service company will not hesitate to accept the VPSHR as a standard of performance delivery. When the VPSHR become part of the company's way of doing business, it will further the long-term goal of broad acceptance of those principles throughout the industry and society.

4.1.2 Overview

Each company should develop and formally sign a Code of Conduct for Security Providers. This public document publicly commits the company and its sub-contractors to uphold basic principles and international standards in the areas of human rights, environment, ethics, use of company resources, relations with government, confidentiality of information, financial responsibility, conflicts of interest, accountability and responsibility of the Board of Directors.[2] The Code is the umbrella document setting general standards of behavior.

The VPSHR will be part of the company standards. However, the VPSHR is not a set of precise regulations, but rather a general set of guidelines open to interpretation. The company should address the ambiguities and clarify what they mean to prevent the private security provider from guessing the intent and measure of success, an unacceptable situation sure to lead to frustration and disappointment for all concerned.

In the security field, a company's contract guard service may already have its own established and published standards. Even so, the company cannot make assumptions as to these standards of conduct without verification.

4.1.3 Discussion

The company's Code of Conduct is the cornerstone document. The company should formally sign, translate and disseminate the document to all stakeholders and publicly post where the company's employees may read it. The Code of Conduct should be a standard part of all contracts and commitments by the company. The company can codify this by adding a sentence stating, "Company requires its contract security service providers to accept and abide by the provisions of the Voluntary Principles on Security and Human Rights as determined and agreed by the two contracting parties."

If the company has an existing guard service contract that does not have these standards included, the company has two choices: (a) change the terms of the contract, or (b) await the next contract extension or renewal. In preparation, the company should declare its intent to require their guard contractor to abide by the standards of the VPSHR. Early compliance will be in the guard company's interests and will give them a competitive advantage over non-compliant competitors. As a first step in contractor compliance, the guard company can provide assurance that its employees are carefully vetted using previous employers' references and whatever other records are available.[3] Weapons are not desirable and as a matter of policy and should not be used by the company's security guards. If armed force is required, that is more properly the province of the public security forces.

---

2 The Code of Business Conduct is a broad-brush statement, with identified links to a substantial number of supporting documents. These may not all be available on the company website.

3 This background investigation is often the best available course of action for entry-level employees, especially in countries where record keeping is unreliable or not available.

Guard service providers should conduct human rights training as part of the basic guard training program. The company may have to provide some of the essential human rights training if the guard service contractor lacks the resources or expertise. In such cases, the company's security personnel themselves may conduct the training or the public security forces of the host country may be able to provide acceptable trainers. The company and the guard contractor should agree on and provide copies of written Rules Of Engagement for the use of force to each guard. The company should also encourage the recruiting of guards from the local population, even if this requires a program to assist employees who have limited educational background to progress.[4] The equipment issued by the guard service provider to their security guards should include basic defensive items.

Most guard service companies in the developing world have no method of managing human rights allegations, recording and investigating such allegations and taking action. This usually reflects the absence of such allegations rather than inattention. The guard contractor's supervisors usually treat such infractions in guard discipline with a warning or, if the infraction is serious, by terminating the employment.

One effective way to address the various gaps in the current standards would be to require an education and training program for the contract guards. One method for accomplishing this is for the guard company to produce a small, pocket-sized booklet issued to each employee and signed by the employee acknowledging he had read and understood the contents. The guard company can then maintain a copy of the signed acknowledgment in the personnel files available for review by the client. Yet another way is for the guard company to print the key points of the VPSHR, the contractor's Code of Conduct and the Rules for the Use of Force on plasticized "smart cards" attached to the company's identity access card. Both the booklets and smart cards should be in English and the appropriate local language for ready reference and inspection.

Developing a similar standards booklet and associated plasticized memory aids, or small wallet-sized cards, is easily within the capabilities of guard service companies. The company can require such training aids as part of future guard contracts. In urgent cases, an incentive payment for early fielding under an existing contract is appropriate and moves the training process forward. There are three ways to do this training:

1. Require the guard service contractor to conduct the training from in-house resources. They may have on-the-shelf training available locally or from their corporate headquarters. This is the quickest way, but the product is beyond the company's control and cost control is difficult. Before selecting this option the company should insist on seeing what the guard service contractor has for resources, such as lesson plans and instructional materials.
2. Require the guard service provider to conduct the training and provide them an approved vendor list from which the guard service company can select the training program that meets their needs and the company's standards. This may be more expensive and time-consuming, but guarantees quality training and allows the same vendor to conduct additional or modified training for the company's employees and the public security forces.

4 The turmoil of the preceding decades in some host country means that most rural persons have had very little formal schooling. This is not an issue directly relating to the VPSHR, but is important for the overall development of the Company Security program.

3. The company can contract directly for the training, use the training team and resources for training the guard force and company security personnel and even conduct relevant training and scenario-based drills for the local public security forces. This may be more expensive and time-consuming, but provides the best overall content control and assures delivery of a quality product to all key parties. In most cases, this alternative is the best option overall.[5]

4.1.4 Recommendations

1. Complete, sign and promulgate a Corporate Code of Conduct for Security Service Providers. Make this document a part of all company contracts. Add this document to the company's website with all supporting links included.
2. Declare to the guard service contractor the intention to include adherence to the Corporate Code of Conduct for Security Service Providers as a contract deliverable in all future contracts or extensions of the existing contract.
3. Require the guard service contractor, and any future security service providers, to develop and maintain internal procedures for investigating allegations of human rights abuse and other criminal behavior. These procedures should be complementary to the company's own procedures, the Corporate Code of Conduct for Security Service Providers and the VPSHR.
4. Require training for all security service personnel in human rights, the use of permissible force, ethical behavior and the VPSHR. This training can be provided by the contractor for its personnel or by a third party contractor who can insure commonality of training among all security providers. Any training provided to the company's security department and contractors should be offered as a courtesy to the police and other public security forces located at or near company facilities and sites.

Advantages

- Establishing and publicizing the Corporate Code of Conduct for Security Service Providers takes the initiative in discussions of business ethics and conduct. It publicly commits the company and its sub-contractors to recognized international standards.
- Early coordination with the guard service provider on an active program to raise the public posture of respect for human rights and ethical behavior should give the contractor a competitive advantage both locally and internationally. It is in their interests to embrace the initiative.
- A training program demonstrates the company's commitment to the spirit as well as the letter of the VPSHR and provides guidance and information to security providers.

Implementation Risks and Mitigation

Greater specificity and higher expectations may increase the cost of contract security services.

4.2 TRUST, BUT VERIFY

4.2.1 Relevance to the VPSHR

The VPSHR work best when all concerned have a common understanding of the expectations and obligations to implement the principles. Including the Code of Conduct for Security Providers and specifically the VPSHR in all contractual agreements with private security contractors is one of the expectations under the VPSHR. Deploying an independent monitor is not part of the VPSHR, but substantially reinforces the entire process and will help the company demonstrate its commitment to ethical behavior.

---

5 If the company selects the third option it should discuss the program with similar companies in the area to see if they would like to share costs on a pay-as-you-go basis. These companies are likely to need this training. The licensing and permitting, course development and deployment costs are a major part of the overall cost.

4.2.2 Overview

The company can require acceptance of the VPSHR in its contracts, but cannot assume they will be fully implemented without verification. Even with the best of intentions, a security service contractor may not interpret the fundamentals of the VPSHR in the same way as the company. The best way to resolve ambiguity is through discussion during contract negotiation and verification, and subsequent independent monitoring.

4.2.3 Discussion

The company's contract with its security provider(s) can specify performance deliverables, but the implementation will require an active supervisory effort by company management. The responsible agent for this supervision is usually the company security department, through the on-site security managers and deputies. Senior management, however, is ultimately responsible for ensuring the organization and its contractors fully meet expectations.

The contract execution of private security providers is best facilitated by explaining to the contractor or bidders the company's expectations concerning the letter and spirit of the Code of Conduct for Security Providers and the VPSHR. This should occur not later than during negotiations for contract renewal or reopening the contract for competitive bid. The company should make clear its requirements for any contract security provider[6] and the methods it will use to verify this performance objective. This will ensure the security contractor is not in the position of guessing at what the company wants.

One effective way to ensure all parties understand the expectations is through regular meetings between the company and security guard service contractor. At these meetings the company security manager should provide the private security company with a monthly performance check. This performance report will contain any contractual issues and concerns. In addressing the VPSHR, the report should include the following elements:

1. Contractor observes company policies regarding ethical conduct and human rights.
2. Contractor has set mutually agreed ROE on the use of force and trained all employees in these standards.
3. Contractor investigates all occasions when force or apprehension of a suspect has occurred to ensure this was done in accordance with company and contractor standards. All such incidents have been reported to the company security manager.
4. Contractor has acted in a lawful manner in performing all aspects of the contract.
5. Contractor has established a policy for investigation of allegations of abusive or illegal acts.
6. Contractor has recorded and investigated allegations of human rights abuse and has provided a written report of the results to the company security manager.
7. Contractor has provided defensive equipment for the guard force as required by the contract and has properly trained the guards in its use.
8. Contractor has conducted background investigations and, to the best of its ability, verified no member of the security force is a known human rights abuser or wanted criminal. Personnel records that validate this requirement are maintained on file by the contractor and available for inspection.
9. Contractor's employees understand they may not limit the rights of peaceful assembly, collective bargaining and non-violent demonstrations that do not violate local laws.
10. Contractor has security guards trained in provision of emergency first aid in the event a person is injured in the course of an incident.
11. Contractor maintains the confidentiality of information gathered in the course of duties.

---

6 While this discussion concerns security providers, it is fully appropriate and highly desirable for the Code and VPSHR to be included in ALL contracts.

12. Contractor has accepted the VPSHR and included them in his training program for security personnel assigned to company facilities or activities.
13. Contractor meets company goals for hiring and training local employees and giving them access to the full range of the contractors' career development plan.
14. Contractor acknowledges that failure to comply with the standards set in the checklist constitutes justification for imposing performance penalties, including termination of the contract.

The company should also include in any security contract the provision for an annual contract audit to verify the charges and invoice procedures. An audit will require support from the company's finance department or the services of an outside auditing company.

An excellent and proven way to validate compliance with contractual obligations and, at the same time, validate the company's performance is by using an external monitor. An external review can also provide recommendations and suggestions to enhance the performance of the security department and other service providers.[7] There are credible, qualified and respected individuals and organizations that perform this function. An external review establishes the effectiveness of the company's security function and observance of the VPSHR. It also allows an independent validation of the company's other contracted service and activities. Internal performance reviews and audits do not carry the credibility of an external and impartial monitor. An external review or assessment is the best method of enhancing company's reputation for proper and ethical behavior. It shows that the company not only talks the talk, but walks the walk. In other companies a credible external human rights review has largely dissipated criticism.

4.2.4 Recommendations

1. Meet with the security guard service contractor and inform them that committing to the VPSHR will be a performance deliverable in the future. Explore early implementation of the expectations of the VPSHR with the security guard service contractor and explain the advantages to the contractor for early implementation.
2. Use the elements above to develop a checklist of VPSHR expectations; use this as an evaluation tool and provide the result to the private security provider each month.
3. Identify a reputable independent human rights compliance monitor; contract for an annual or bi-annual review of security and human rights practices.

Advantages

- Early discussion and clarification of delivery expectations will permit the security guard service contractor the opportunity to adjust their contract of services and identify any added costs that may result.
- A checklist will help company security managers and deputies to apply a common standard at each site and permit both company and security guard service contractor with a written track record of compliance with company's standards as defined by the Code of Conduct for Security Providers and supporting policies including the VPSHR.
- Independent validation of the company's implementation of the VPSHR and its Code of Conduct puts the company on the moral high ground. It can also make recommendations on additional steps to improve security and human rights practices.

---

7 While full transparency is desirable, the report should be released only after careful legal review by the company's legal staff. The scope of work and terms of reference should be specific about references to the host government and peer companies.

Implementation Risks and Mitigation

- The company can expect additional costs for additional services in the security guard service contract. An effective VPSHR implementation program will require additional resources and internal adjustment by the security guard service contractor. For example, the guard contractor will likely have additional training requirements for their own staff and supervisors. The company may have to accept modest additional contract costs to achieve the new standard.
- Private security service provider(s) may not have the training or experience to effectively meet company's expectations. One way the company can manage this issue is by specifying required standards of performance in the Invitation To Tender (ITT) contracts for guard services (and all related security services). Companies that want to remain competitive will adopt the VPSHR, spreading the principles across the private security industry.
- Contracting an external and independent review carries an expectation that the findings and result will be addressed. There may be pressure to publicly release the results of such a review. As with other security related documents, transparency is highly desirable. If some parts of the review proc-

Stakeholder Engagement

The VPSHR encourages and expects that *"Companies should consult regularly with... civil society to discuss security and human rights."* Consultation is the start of the engagement process that leads to effective issue management. Without a consistent and coordinated plan, the company will eventually find itself at odds with one or more critical participants in the security environment.

Stakeholder consultation is a well-established component of the social and environmental impact assessment and management process of most major projects. The VPSHR introduce this as an element in security management, where it is a less well-established practice. Effective stakeholder consultation with respect to security and human rights draws on the same basic principles as for engagement on wider environmental and social topics.[1] Stakeholders need to be identified; appropriate engagement processes started with the understanding that these will develop over time; the interests of different stakeholders understood; and, where possible, collaborative solutions found to shared concerns. The discussion in this report focuses on stakeholder engagement in the context of VPSHR implementation.

5.1 THE STAKEHOLDER ENGAGEMENT PROCESS

5.1.1 Overview

The need for communication, dialogue and issue management (referenced as Consultation within the VPSHR) is often considered an easily understood requirement of the VPSHR and yet is many times under-managed. A company's engagement process on security should reach out to, and include, all communities and interested parties, and support constructive interaction among them. The company should be on guard to prevent manipulation of the consultation process by those with a narrow or self-serving agenda. One way to curb this is to provide training for the communities and prepare them to understand and participate in the consultation process. Consultation is the starting point for effective management of sensitive issues. To be effective, consultations should identify and clearly understand the concerns and shared interests associated with responsible resource development. Typically, this is managed through a combination of bilateral meetings and multi-party sessions. Small groups (six or less) often can tackle real problems and achieve consensus. Larger groups serve as sounding boards and help reinforce the principles of shared interests and concerns. Regardless of the types of engagement activities and tactics undertaken, it is critical that the parties understand and agree to what can be expected from the engagement process. For example, where is engagement primarily about information sharing? Or aimed at joint problem-solving?

Company management should decide its core interests with respect to stakeholder engagement regarding security, and clearly communicate these. For the security function, it is important to reinforce that the security of the site and the surrounding communities requires a compact among the involved parties to work in collaboration to the benefit of all. One way to phrase this is "We All Share Responsibility for Success" with success defined as a safe and secure workplace and surrounding environment, insofar as the company affects this.

1 See, for example, the IFC Good Practice Guide to Stakeholder Engagement, on *www.ifc.org/ifcext/enviro.nsf/Content/Publications_GoodPractice_StakeholderEngagement*

5.1.2 Discussion

The first step in the engagement process is to determine the stakeholders. For this discussion, the report identifies six key security stakeholders involved in the success of the company. This is an illustrative example, not a fixed rule. In some situations, there may be other identifiable security stakeholders. These might include investors, labor unions, and distinct sections of the community such as youth groups, women's cooperatives or other institutions. A careful analysis of the area of operations will be helpful in identifying the key security stakeholders. Unless the number of participants is limited, however, it will become unwieldy and dysfunctional. Each stakeholder has affiliates and adversaries among the others and may not always cooperate fully for their own reasons. If the company is to achieve a stable security environment each stakeholder needs to perceive that its interests are important and its concerns heard in the engagement process with the company. (For example, traditional village leaders may have disenfranchised women's groups. The company can advance the overall security agenda, reduce violence against women, and promote a more stable society by responding to their particular concerns.) A goal is for all stakeholder groups to recognize that the company is making good-faith efforts to address their respective equities within legal limitations. Compromise is an essential element in consultations. All stakeholders share the responsibility for security; this is not the exclusive province of the company, the government or the security services.

The matrix below illustrates an analysis of the responsibilities of different stakeholders, the leverage they bring to the security process and their implied interests. Each stakeholder group is discussed further in the sections that follow.

Stakeholder	Responsibility	Leverage	Interests
(1) Company Management	Financial, technical and operational.	Budget, work force and project controls.	Efficient, effective, profitable operations; protect company reputation.
(2) Local Communities	Maintain basic level of law and order.	Labor force; obstruction, disruption and protests.	Economic improvement. Minimize negative social impacts.
(3) Government	Provide legal and regulatory reliability.	International recognition, legal and regulatory authority.	Economic advancement and development; a stable revenue stream from project operations.
(4) Police	Maintain Law and Order.	Legal authority to enforce law and make arrests.	Demonstrate abilities. Improve capabilities and professionalism.
(5) Armed Forces	Defend the nation.	Legal application of coercive force.	Increase professionalism and protect reputation.
(6) Non-Governmental Organizations (National and International NGOs)	Monitor, investigate and verify proper practices; support implementation through cooperative initiatives	Publicity, courts, demonstrations and disruptions.	Protect and enhance their cause(s).

1. *Company Management*. The senior site manager will have to make decisions for security reasons that will cost time and money. To fulfill the mission of operating a safe, profitable and efficient operation, he has considerable authority to allocate resources, make decisions and determine what is permissible to address the other stakeholder's expectations. In addressing these expectations, he should make full use of his staff, particularly the security and public relations staffs. The test of a successful security regime and the maintenance of business continuity is effectiveness rather than minimizing costs. For example, where there are ongoing exploration activities in remote areas, company management should be sensitive to the precedent these activities will set and expecta-

tions they will raise. The company should conduct a Risk Assessment prior to beginning activities in a new area. Part of the threat mitigation process will be to involve the community relations and security department in the initial contact and coordination with the various stakeholders.

2. *Communities.* No company should ever assume that it can "buy" goodwill and thus inoculate itself against local discontent. The local communities in the immediate area of the site and in the surrounding region will approach the site as an opportunity to secure benefits to them (jobs, compensation, education/training, public services) for as long as possible. Local communities are potentially the greatest asset and the greatest threat to the company. They are the key to success or failure. To be successful the project should make every effort to establish a mutually respectful and beneficial relationship with communities that includes linking tangible benefits such as jobs, development and economic improvement with the safety, security and success of the company's operations. It is vital that the community understand that these benefits cease if the company is unable to operate.

3. *Government.* Local governments usually have limited capacity and ability to deliver services in remote, under-developed regions where many major projects are located. Centrally funded public services (health, education, communication, justice) are often minimal. The company should adjust its own expectations accordingly and may find it beneficial to promote government capacity-building projects, especially those conducted by recognized international donors. The best way to provide funds when working with host governments is through matching funds rather than by grants or donations. This empowers the government officials and gives them 'pride equity' in the capacity building process.

4. *Police.* Police in the developing world are chronically under-resourced, under-equipped and under-trained, at least to the level they would wish. This does not mean that they do not aspire to be competent and professional policemen. Government security forces are the final protector of the company operation. An accurate assessment of their capabilities is essential. As with local governments, the company may find it in their best interests to help build capacity within the local law enforcement agencies, particularly through existing international police assistance programs. (Additional methods for doing this are discussed elsewhere in Section III, Relations With Public Security.)

5. *Military Forces.* In addition to national defense, the military forces of developing states usually have a constitutional role of providing assistance to the civil power. In practice, this usually means they are concerned with local political stability. A military unit will often be stationed in the area of the company's site, and a regional military reinforcement capability will be a vital component of national security and thus of the company's security system. The military forces of the host country usually prefer to stay out of providing local security as long as the police are capable of doing so. However, the military forces will still have a role to play; the company should never ignore them. The company should invest the time and effort to build an appropriate, continuing relationship with the military. (See Section III, Relations With Public Security.)

6. *NGOs.* Responsible non-governmental organizations have an enormous, generally positive influence on multi-national corporations and on conditions and activities at a site. NGOs are invaluable in documenting, in a neutral and credible manner, the social agreements and understandings with local communities and helping these communities build their management capacity. Early consultation with a range of NGOs will serve all interests, allow the NGOs to participate in social planning and environmental impact and make use of their expertise. Having responsible national and international NGO advice will help protect the reputations of all other stakeholders and may serve as an honest broker when allegations of abuse or illegal activity surface.

To ensure the company mobilizes its resources effectively, it should have a specific engagement

strategy for each security stakeholder group. The community relations department is an important part of this engagement strategy. In some cases, they lead the interaction (with the local community, government and NGOs for example). With other stakeholders, they support the effort and assist as necessary (with police, military and company employees). The company should not engage in practices that stakeholders could perceive as manipulative or divisive and should ensure that its stakeholder engagement conveys a consistent message to all stakeholder groups with respect to company interests and approaches.

The matrix below provides an example of key company messages and methods of engagement for each of the six major security stakeholder groups at the beginning of a project.

	Employees and contractors	**Government**	**Police/Military**	**Communities**	**NGOs**
Key company messages	1. Each employee is an ambassador for the company. 2. The company will obey the host country's laws. 3. All employees are part of the security system that protects you and the Project. 4. The company needs employee's comments and help to head off problems.	1. The company cannot succeed without you. 2. We can jointly manage success and development. 3 We need to both have realistic expectations of the other. 4. Join us to build local capacity.	1. Eyes of the world are on the host country and local site. 2. We all share the responsibility for success. 3. All parties should understand the responsibilities of the al the others. 4. This is a strategic development; everyone should take the long-term view. 5. Voluntary Principles are critical to us all.	1. The company is a business and will do things that make sense as a business. 2. The company is a neighbor – and wants to work together with the community. 3. The company cares deeply about health and safety – both on site and in the community. 4. The company needs your feedback and support on security issues.	1. The company wants to work with you to achieve progress. 2. The company needs share its expectations and dialogue with all responsible parties.
Method & Medium	1. Security web page. 2. Standardized Workforce Induction video. 3. Security Code of Conduct. 4. Present a security moment at all meetings. 5. Management workshops. 6. Tip line telephone number to security and suggestion box in key locations. 7. Tip Box in common use areas.	1. Regular meetings with custodians of the relationship(s). 2. Work all levels – local to national. 3. Host orientation visits. 4. Interface on regular basis and coordinate with Community Relations on key messages. Make sure the messages are mutually reinforcing.	1. Regular meetings with each echelon. 2. Offer capacity building training. 3. Monthly sports event. 4. MOU on standard operating procedures and expectations. 5. Share the VPSHR and clarify company commitment to highest standards.	1. Community Relations has the lead. 2. School programs (safety, security, health). 3. Posters on living, such as "How to get a job". 4. 'Comic book' visual orientation on the project. 5. Publicize 'Redress of Grievance' procedure. 6. Bulletin boards in each community. 7. Community Security Forum. 8. Radio program.	1. Community Relations leads interaction with local and international NGOs; Security supports. 2. Map key NGOs concerned with security and human rights issues. 3. Monthly bulletins. 4. Security page on the company website (updated monthly). 5. Hotline to Social Investment for questions.

Key Messages

An integrated and coordinated message set is relatively easy to create, but is often missing in engagement programs. One size does not fit all. The company's outreach program has to be both consistent and credible. An extractive industry should be especially careful of slipping toward an artificial image of altruism. This is unsustainable. Extractive industries are for-profit businesses and should not shrink from stating this openly and clearly. This fact is obvious and honorable. As a function of this stand, the company's social investment programs should have a direct, or at least indirect, linkage to the success and productivity of the company. Philanthropic projects are not a core competency of extractive industries. Local NGOs, international donor organizations and foreign governments have both the charter and experience for development projects. The company can and should engage in social investment projects that are sustainable after the company is gone and are of value to both the community and the company.

A company should transmit the clear message that it is a *partner* in the development of the local community and region. The company will prosper and share the benefits with the local communities, if all the other partners accept and *share the responsibility* for safe and secure operations. Shared responsibility is the core of a community-based security regime. Understanding this message and making it part of the company's core values begin with the company and its workforce.

Company

The company's own workforce is the best method of transmitting its message and getting feedback from the community. The workforce, both national and expat, have enormous impact on the host region and the populace. Collectively, they should have access to the Voluntary Principles and the company's core ethical standards. The company can transmit this core message of ethical and moral fairness, transparency and accountability in a variety of ways. These include, but are not limited to, (a) the morning safety briefing (sometimes known as the toolbox meeting), (b) posters and handouts and (c) nominal give-away items like coffee cups.

Management, including expatriate management, is the key to effective security just as they are critical to the safety culture of the operation. They should understand that they represent the company to their subordinate workers. Line management should understand they are part of the security system that protects them and the company. Firstly, they should avoid creating a threat from the workforce by inappropriate behavior. Secondly, they have the responsibility to sense unusual situations, worker tensions and things that just seem out of the ordinary and inform the security manager. This includes inappropriate behavior by public security forces on site and in the immediate area of the company's operations. The engagement of management also includes the security and social development managers.

Scenario 11: Recognition of Effort

In one project, a grass fire threatened the company base camp. Off-duty security guards took the initiative to grab shovels and fight the fire, putting it out and saving the local forest area and base camp from burning. Each guard was presented with a special recognition letter and cash payment by the project manager, was photographed with the project manager and given a signed print, and was given a small special merit pin to wear on his uniform as a mark of distinction. This would also be an ideal time to present a recognition item with the company's key message – "Shared Responsibility" – that the employee will wear proudly when he is off duty. The community can identify with its employed members and with the need for the company to maintain its business continuity.

For Discussion

How does your company recognize and reinforce excellence in the prevention of escalation of incidents?

Usually they will become aware of an issue before anyone else. The company cannot turn a blind eye to human rights misdeeds that come to its attention.

All avenues for reporting allegations should be available to employees. These include, as a minimum, a security phone number for tips, a web address, a mailing address and suggestion boxes at common areas such as the dining hall and site entrance.[2] The company has a greater ability to influence its own workforce than it has with the other security stakeholders. Unfortunately, many companies ignore this valuable asset and proceed on the assumption that employees inherently understand the company's values, its contributions to the local area and see their own interests as identical to those of the company. This can be a false and dangerous assumption. An effective way to transmit the company's message is through an induction video[3] for all new employees and all visitors to site. This will ensure all hear consistent messages.

One way to enhance the impact of local benefits and align the company, the workforce and the community is to allow workers to participate in community development projects. The company can do this by giving them time off to participate or pay overtime if they participate when they are off-duty from their regular shift.

The company cannot forget that it has considerable leverage over its contractors. Certainly, the security provider should be a conduit for implementing the company's VPSHR program. (See Section IV Relations with Private Security.) Other contractors, however, should be required to accept and conform to the company's Security Code of Conduct.

Government

The lead for engagement with local and national government is with the government relations function. At the national level, the company's representatives in the capital should manage this relationship. The company will want to nuance the message it communicates at each level. The company should use both its own expertise and consult others with experience in the host country culture, laws and social practices to develop the details of the message. At all levels, however, the key is regular and frequent meetings to share information and insure mutual understanding. The company should host selected government officials and staffs on orientation visits to make the company's operational site(s) a "real place" and not just a remote point on a map.

National-level interaction requires corporate senior leadership. As part of that effort, the company will be sharing the understanding of its obligations under the VPSHR. Ideally, the government will see national acceptance of the VPSHR as an example of the international good practices that support the host country's aspirations. As good governance gains strength, international confidence and investment will continue and accelerate. The VPSHR are consistent with commonly accepted international standards established in various United Nations protocols. Many developing countries, including Indonesia, Turkey, Georgia and Azerbaijan, have included the VPSHR as part of their contracts with international companies. At the national level, however, it is important that corporate management develop rapport and a degree of mutual confidence with their host-country counterparts. If the central government does not accept and give at least tacit support to the VPSHR, gaining traction at lower levels will be infinitely more difficult. To gain that support, a company will have to invest its political goodwill on the issue.

---

2 While some of these means may seem of marginal utility, tips can come from many sources, including national and international NGOs. Further, the cell phones and internet access is now very widely available, even in remote locations.

3 It will be necessary to have this presentation in the local language as well as English.

At the local government level, in countries with devolved government functions, the company should seek to negotiate a protocol agreement with the regional or provincial government to clarify expectations. The issue of the company's VPSHR policy is closely rooted in governmental capacity. At this level, the message is one of mutual reliance. Neither party can succeed without the other. The area cannot attain its potential and attract responsible investment without strong institutions. Some extractive industries may come because they have no choice if they are going to exploit local resources. Attracting investment from other, competing locations is the key to real broad-based success. This requires infrastructure, trained local labor and security. International companies can help with all these, in collaboration with the local provincial authorities. Working with government is an effective way to multiply the positive effects of a company's operations. Joint planning, cost sharing, regulatory reliability and workforce mobilization can enhance the government's equity and support in development. Where possible, the company should seek ways to make schools, clean water projects, health services and other social investment a multi-party strategy. It is better for the company's long-term interests if it is the second name on a joint government-company project rather than first on a philanthropic donation. At the local level, the company should recognize that governmental capacity is limited. Local social institutions often take the place of, or *de facto* are, the only effective local government. The social control mechanism in developing societies is fragile. Local traditional leaders can be very effective, but these key people are vulnerable to a loss of influence because of the population influx stimulated by the company's economic activity.

Scenario 12: Social Controls

One project operated in a remote venue, near a small village of 350 people. During the earliest consultations, the villagers expressed concern about "outsiders" coming in. The project created several protocols to manage employment, limit imported workers and discourage in-migration. Before construction even began, however, the village expanded to over 600 people, including sex-trade workers, small-business people and other elements. The newcomers were largely from a different ethnic group and religion. All this occurred despite the fact that the local traditional leader had virtually absolute control of in-migration through his control of resident identity cards. In this case, the traditional leader put self-interest over the good of his group. The result was that residents were fast becoming a minority in their own village as outsiders flooded into the area.

For Discussion

How can the company help the community and local government build capacity to manage a population influx and limit results for the company's activities?

Public Security Forces
(Police, Military and National Intelligence)

The company's security department is the lead for maintaining the relationship between the company and the public security forces. Since a major section of this document has focused on the public security forces, this discussion will be brief.

The best approach to public security forces is a direct appeal to the visibility and prominence that the company's operations bring to the host country. While the company cannot assume or reduce the responsibility for security that falls to the police and, by extension the military, the company does share that responsibility. The company should periodically recognize and share credit with the public forces for successful, incident-free operations.

Communities

The overall engagement process involving local communities is the responsibility of the community relations department. This department should be the custodian of the grievance and dispute resolution mechanism. The community may have a number of issues that require company attention, but are not security related. Left untreated, however, community grievances will often manifest themselves as security problems. For this reason, the security department will need to interact with the communities on a regular basis. Security should always do this in coordination

with community relations. The relationship between the company and the local community is critical. That relationship is the jugular vein of a company's operations. It is vital that the foundation of this relationship is built on more than goodwill.

Security consultations with the community are fundamental to a strong security system. There are two methods well suited to this: a small Security Working Group (SWG) for problem-solving and a larger Community Security Forum (CSF) for information-sharing. Both have a role to play in making sure the community has the opportunity to bring forth their concerns about the local security impact of the site's operation. Consultations are two-way discussions, not a bartering for additional concessions from the company. The company security department will track every issue raised in these discussions and, when resolved, ensure the relevant company and community leaders sign off that the issue is closed. The best term for this listing is the issue tracking log.[4]

In some cases, the issues entered in the tracking log may simply be requests or comments for follow up. This register is a tracking tool to maintain focus, nothing more.[5] In some companies, an issue tracking log has taken on the character of a contract, an inventory of deliverables or a scorecard. This establishes a counterproductive demand/response relationship between the participants. The tracking system should be a part, but not the centerpiece, of consultations. Above all, the company team should understand the dynamic of commitment-making. There have been many examples of a local community misunderstanding an off-hand statement of empathy or awareness by a company staff member, consultant or visitor as an offer to take action on a problem. Often, those present fail to capture such comments in the tracking log. Meanwhile, the local community has lodged the 'commitment' in its oral database, ascribing the company's failure to deliver as a sign of bad faith.

Security Working Group

A (SWG) can be especially effective in taking on and resolving specific issues. Its membership should consist of a representative from the company (usually the security manager), the police chief, the military commander, the local head of government and one or two local leaders. These last positions can rotate so that not only local traditional leaders but also other key opinion-makers have a periodic opportunity to participate.[6] In some cases, local leaders have abused their position to control access to the company and the grievance resolution measures that are there for everyone's use. The Community Security Forum and townhall venues can act as a check on this tendency. The company can also make its activities known through public announcements, posted on community bulletin boards. Ideally, a neutral moderator should chair the Security Working Group meeting.[7] If necessary, the company may have to act as host. The SWG should meet monthly until the participants and security conditions dictate a different frequency. The SWG will be most effective after the members have built mutual trust among themselves to take on issues openly and work together on solutions. This will require a degree of confidentiality to achieve results acceptable to the larger community. Issues can be tabled, discussed frankly and solutions proposed by the members. If the inter-personal chemistry

4 Not a 'complaint log', because every issue will not necessarily be a complaint. The term complaint log carries a negative connotation.

5 Tracking lists are a common management technique in industry. In the developing world, where there is an oral rather than written tradition, communities may not understand the concept. Such societies often distrust written documents. These documents very rarely carry the same acceptance in an oral society as they would in a western context.

6 This is important. The local government representative can act as spokesperson for the civil community, but at least two other local leaders should attend to keep the playing field level and allow the community more than one voice at the table. By rotating the leaders in attendance, the company can minimize the potential for factionalism and collusion.

7 Often the local university, if one is reasonably nearby, can provide a trained moderator. In the absence of any other person, a church or other religious organization may have someone able to fulfill this role. The moderator must be able to guide the discussion, act as honest broker, but not become a partisan participant.

works in this group, they can achieve real results. The SWG empowers the community without indicting the public security forces or the company. As such, the topics should not be restricted to mine-related issues. The moderator is crucial to keeping the group from deteriorating into a “complaints window”.

The Security Working Group can build on the foundation of any regular security meetings that may be part of the company’s security department and the various local public security forces representatives. While there will always be a requirement for bilateral discussions between the company and law enforcement, the SWG should be encouraged to gradually assume responsibility as the action agency for most routine security issues. Over time, the scope of bilateral communications can then narrow to technical coordination on law enforcement issues. The SWG is fully successful when it can collectively anticipate, address and resolve security concerns before they become threats.

Community Security Forum

A Community Security Forum has an expanded membership that includes representatives from the security stakeholders and other key opinion-makers, including additional traditional leaders. Other representatives could come from youth and women’s groups and any other appropriate functional group. The membership may fluctuate, but a manageable number is about 12 to 18, meeting quarterly. This group can table agenda items, receive information of a general nature concerning mine developments, discuss concerns and participate in the discussions. The Forum absolutely requires a respected chairman who can maintain order and keep demagogues from hijacking the agenda. The Community Security Forum is a consultative body, not a decision-making one. It can be an effective venue for raising community issues. If the moderator does not keep a tight rein on the agenda, there is some risk that the CSF will become overly emotional and confrontational. This is one reason to keep membership within manageable numbers.

Townhall Meeting

An open townhall has much merit, if it is within the cultural heritage of the community. A townhall can be a foreign concept and, if the moderator is not well prepared, can have negative consequences. The community relations department should conduct this open meeting. The purpose is to share information while not undercutting the role of the traditional leader as community spokesman.

Other Means and Methods

A number of other effective ways exist to transmit and reinforce the company’s core security message. For example:

1. *Sports Leagues*. Providing modest sporting equipment, like soccer balls and jerseys, is an excellent initiative. Providing these printed with the company’s key security message – e.g., “Shared Responsibility for the Security of All” – is better. Sports leagues are sustainable, inexpensive and effective ways to build confidence, leadership and trust. The company should field its own team(s), including one from the security force, to play teams including from the police and military.
2. *Cultural Performances*. A local musical group can be used to good effect by the company. The theme of their performance should be more than simply goodwill, but rather the reinforcement of the core message(s). This, and possibly other groups, can be extremely effective in the company’s social investment programs.
3. *Frisbee Give-Away*. The Frisbee is an easy toy to use and play with. It does not need additional equipment, a large playing area or much training. All ages are entertained. Frisbees, printed with the company logo and the core message, chould be a “prize” of choice to be handed out at all appropriate occasions. Frisbees are relatively cheap and durable.
4. *Photographs*. People in developing countries have little occasion to have their pictures taken. The “grip and grin” photo should be a staple of community interaction events. Project sites can easily obtain the capacity to take digital photos, print and laminate them. The community relations and security departments should have small digital cameras issued and carry them at all times. A group or individual photo, presented within a day or two of an event, is of priceless impact.

Non-Governmental Organizations

The human rights NGO community, both national and international, is a security stakeholder. They should be included, in any event, and are a danger if shunned. The company has a stake in getting its side of the story out to media, advocacy NGOs and concerned people. Responsible NGOs will usually work with socially responsible companies to address their special concerns and equities. Often this will be possible only under conditions of confidentiality. If the NGOs' conditions for mutual consultation are that these be on a non-attribution basis, the company should agree. Security issues will be an important concern of human rights NGOs. Therefore, the security department will be active in dealing with these NGOs and assist in forging a company/NGO relationship of trust.

The core message from security to human-rights NGOs is: *We want to work with you to advance the respect for human rights in our area of operations and beyond*.

To achieve progress, the company should commit to transparency, which means pushing information to those concerned if there is a security incident. Following security incidents, the information provided by the company must be factual. When warranted, the company should admit its mistakes, identify those accountable and list any corrective actions underway. Ultimately, NGOs will respect and have confidence in the company's intentions if the company is candid and honest. In meetings with NGOs, the company should include the security manager as a member of the delegation. Let the NGOs hear directly from the person responsible for security operations about the situation on the ground. The security manager should carefully research the facts for these sessions. A note-taker can record any unanswered questions and insure the company provides a follow-up answer.[8]

A positive method for handling security information to the greater audience is through the company website, if it has one. The company homepage should have a security section as part of the drop-down menus. This webpage should include all security-related documents and agreements in the public domain. It should also identify a contact location for security-related questions and inquiries. In addition, the web address, mailing address and telephone hotline number should be included to report allegations of human rights abuse.

5.1.3 Recommendations

1. Initiate an aggressive consultation process individually tailored for each of the several security stakeholders.
2. Coordinate this effort so that the messages are consistent, mutually supporting and honest.
3. Manage this effort through a monthly checklist or matrix of contact opportunities and commitments.

Advantages

- An effective engagement strategy will defuse much misunderstanding and harness the efforts of each stakeholder in supporting the efforts of the whole to maintain and strengthen the security environment of the company's operations, and also that of the community and the country.
- This effort takes the initiative to detect and deter problems rather than waiting passively to react to them.
- This establishes the VPSHR as the common policy link among all concerned with security, human rights and transparent operations.
- It addresses all stakeholders, not just local communities.
- A security webpage can offer a venue for reporting allegations of human rights abuse.

8 The credibility of the person on the spot is irreplaceable. NGOs and media are skilled at spotting a phony or a mouthpiece. The security manager may require specific media relations training.

Implementation Risks and Mitigation

- An engagement program is time- and resource-intensive. Most companies already have established the main elements, however. The company should gather these elements together within a single strategy and set clear goals, with the supporting tasks to accomplish those goals, for each responsible person.
- The stakeholders will become frustrated and lose confidence in the company if it does not lead the engagement process satisfactorily. The company will want to exert strong leadership to insure this does not happen.
- The local community can misconstrue statements by well-intentioned visitors, consultants or other company-affiliated persons as commitments by the company. Management workshops with company employees as well as briefings for consultants and visitors, are effective ways to manage this challenge. In the community, the company can address this potential problem by reinforcing in advance *exactly* who has the authority to make promises on behalf of the company.

Resources

The company's strategic communication plan is the basis of the consultation process. If the company does not have a strategic plan, it should contract for a subject-matter expert and hold a workshop to develop one. The company should give final approval for the strategic communications plan and consultation program at a meeting of the senior management officers. This issue is too important to delegate. A failure in communication or consultation can cause significant harm to the company's operations and long-term damage to its reputation.

5.2 COMMUNICATE THE STANDARDS TO ALL STAKEHOLDERS

5.2.1 Relevance to the VPSHR

Open communication is fundamental to the VPSHR. The VPSHR recognize that some information should remain confidential, particularly as it relates to specific individuals or if it could put people at additional risk. As a rule, transparency offers more advantages than dangers.

The hallmark of a successful security program is open and effective communication with all interested parties. In so far as possible the company should communicate the standards of performance for the private security provider to the security stakeholders. Each has an interest, and several are vitally concerned, with the way the private security guard provider will behave. The more transparent this is, the less cause for confusion and misunderstanding possibly leading to confrontation and conflict.

5.2.2 Discussion

As the company develops its new relationship with the private security contractor, some aspects will become visible. There will be more training on site concerning the standards of behavior. The guard force will become more visible and the police will be less visible as they move to the reserve, back-up role. Some additional equipment may make its appearance. Unless the company explains the reasons for these changes, the changes can easily be misinterpreted.

The company workforce at a site will be among the first to notice the changes. As soon as the company makes the decision to implement a change, it should inform its employees about that change and the reasons for it. This information process is part of a security awareness campaign that publicizes the goals, objectives and shared responsibilities for security at the site. For example, the Rules of Engagement should be printed and posted on the walls of all security guard facilities and in common access locations. This measure will inform all employees of the standards of behavior for the guard force.

Changes in the posture of the security program will affect the community. They will hear rumors of

the changes and may become apprehensive. The community is vitally concerned about local hiring opportunities, potential changes in the social development structure and programs, realignment of responsibilities between the company's guard force and the public security forces. For instance, when the police are relocated this may benefit, or disadvantage, the local communities. All these factors justify a consistent and complete explanation of what is happening and why. This will help the community understand the impact of these changes on their lives.[9]

Government representatives at village and town level are important parties in the evolution of the security paradigm for the site. Realignment of police stationed at the local site and other potential changes are critical to the local government administrator. Like other officials, he will prefer that the company not make decisions that take him by surprise. Early communication and coordination will pay dividends. The possible expansion of any existing informal meetings into a Community Security Forum will be of considerable interest to him. The company should make every effort to explain the function of that organization and show how it will *benefit his efforts* at good governance.

The police also have a stake in the successful provision of security to the local company site and its operations in the area. The changing security paradigm will offer the police opportunities for enhanced professionalism. This should put the local police command in a favorable light and strengthen their reputation in the community and with their chain of command. Consolidating the police, providing assistance in developing good Rules of Engagement, opening up additional training opportunities, and possibly augmenting their equipment are all highly desirable developments. The company should inform and involve the police in ways that do not imply any lack of confidence or dissatisfaction with their previous performance. The company is simply committing to make the security situation better for all, a situation for which the police will receive the credit.

The company cannot ignore the military and other state security forces. While their focus is mainly on early warning and preventive actions, the security requirements of the company's site will dictate their deployment and responsibilities, at least in part. Therefore, the company should expect to consult with them. For example, changes to the company's security profile may allow the public security forces to focus their scarce resources on more pressing problems elsewhere. In presenting this to the military and the state security forces, the company should assure them that the changes are for the betterment of security in the community and at the company's site, a common goal of all public security forces.

Finally, the company should inform the national and international NGO community of developments in the provision of security for company facilities and activities. This should occur after the local stakeholders have been informed and educated on the changes. The company will determine the venue and timing of briefings to concerned NGOs in accordance with its existing relationship with them. The more transparent and forthcoming the company can be, the better.

5.2.3 Recommendations

1. The company should openly inform the workforce of the proposed and directed changes in the company's formal adoption of the Code of Conduct for Security Providers and the VPSHR. Posters are an effective way of sending a simple message about the workforce's responsibilities.
2. In succession, the company should make the main points that are involved with the VPSHR and the other changes that may result developments known to the local community, police, government, military and the state security forces. The company should inform NGOs as well, *after* the other stakeholders.

---

9 The formation of a Community Security Working Group, discussed elsewhere, will often provide a new opportunity for communities to participate in their security. This can be a very positive and reassuring development for people who have been at the mercy of instability for decades.

3. The company should announce and post details of security changes on the company website and communicate these changes to other appropriate parties as determined by company management.

Advantages

- Open communication reduces misunderstandings and lowers apprehension.
- Information sharing builds confidence and trust with the stakeholder audience.

Implementation Risks and Mitigation

- Some stakeholders may misinterpret the changes negatively. The many consultative methods recommended elsewhere in this document should be sufficiently effective to manage this issue.
- The private security provider may be uncomfortable about releasing some information, such as the ROE. Nonetheless, the company as the contract holder has the authority to require transparency and full disclosure. Responsibility and accountability must be clear before an incident.

Resources

The cost of stakeholder consultations is negligible as a part if measured against the company's normal obligations to be transparent. The security and social development departments will conduct much of the coordination as a routine part of their liaison and outreach responsibilities.

Integration of the VPSHR into Management

The Voluntary Principles on Security and Human Rights are not a compliance document or regulation. There is no litmus test or certification process that validates a company has demonstrated its commitment to faithfully implement the VPSHR. This is a judgment call, made by the company, the stockholders, industry analysts and the security stakeholders and validated in the court of public opinion.

The VPSHR are of no value to a company unless they become part of the corporate culture. Several early signatories of the VPSHR have demonstrated a strong commitment to embedding the values of the VPSHR into the range of their commercial activities and relationships with host governments.

If the VPSHR process is to work in a company, the commitment of the CEO and Board is the critical success factor.

Integrating the VPSHR into management is a long project. It will require committing time, attention, leadership, budget and other resources. The company can demonstrate its integration of the VPSHR into its management systems in a number of ways.

6.1 TIME-PHASED IMPLEMENTATION PLAN

Initially, the company should take the high-priority steps necessary to field a successful program. This begins with a public commitment to the VPSHR and prioritizing those measures that take longer preparation and implementation planning:

1. Make a strong, public commitment by senior management that the company is implementing the VPSHR because it is in its interest to do so. The VPSHR will be a part of the corporate culture of the company.
2. Identify and make those policy decisions necessary for effective implementation.
3. Designate at each management level the persons directly accountable for implementing the VPSHR in their respective organization, activity or function and link this to their performance goals.
4. Appoint a corporate VPSHR champion (program manager) to take staff responsibility for the VPSHR Program and allocate an adequate budget. The champion should report to a board member who carries the VPSHR as part of his or her oversight portfolio of responsibilities.

In the intermediate period (six to 18 months or less), a number of actions are feasible to complete:

1. Lead the interface engagement with host government and communities affected by the company's activities.
2. Provide the necessary resources in personnel and budget to sustain a realistic program that reaches all security stakeholders.
3. Complete and sign the supporting policies, plans, procedures, processes and protocols.

Over the longer term (18 to 36 months – preferably sooner) company management can fully embed the VPSHR in the company's way of doing business:

1. Lead the education and training effort required to make the VPSHR an embedded core value in the company wherever it operates.
2. Communicate the standards and expectations throughout the company to all employees.

3. Establish performance metrics to measure progress in implementation of the VPSHR.
4. Ensure there is an effective reporting mechanism for internal action decisions and external transparency.

No program will be effective without buy-in from all levels of management to make it work. At country and site level, the company will need to translate the corporate directive into immediate action. This means establishing the mechanism to deliver VPSHR implementation. The steps to do this are, in priority:

1. Form Site Security Committees at all operational sites. Form counterpart committees at the country level where there are multiple sites, and at the company's main headquarters location.
2. Identify those measures that should be done at each level and assign specific responsibility for each by phase.
3. Define for each subordinate manager his responsibility and accountability for implementing the corporate ethics, security and human rights policies and clearly link this to the individual's performance plan.
4. Commit the time and management personnel to training so there are the skills and understanding to make this program a reality.
5. Identify and report issues, gaps and progress.

The value of the VPSHR is that they can provide practical guidance for preventing a security and human rights event, and direction for mitigating the event if one does occur.

6.2 PHASE ONE: CORPORATE COMMITMENT

Implementing the VPSHR is in the company's interests and fulfills a responsibility to its stockholders, its employees and to the countries where it operates. The Voluntary Principles are good business principles. Full integration of the VPSHR begins with a commitment to ensure they are reflected in the corporate culture of the company. The company's successful business practices will give it the visibility and prominence that demand an excellent program of ethical and social responsibility.

To be credible throughout the organization, the CEO and Board of Directors should make a strong personal and public commitment to incorporate the VPSHR into the core values of the company.

Amalgamating the VPSHR into the corporate culture will be effective when done through a series of visible implementing steps. The company should publicly announce these steps and post them on the company website. The policy statement will be of interest, but the supporting actions will conclusively demonstrate corporate commitment.

6.2.1 Discussion

If senior management does not completely understand and fully support the VPSHR, other efforts to demonstrate commitment will be hollow at best. Getting informed buy-in from senior management provides the best chance to avoid mismanaging a major incident.

6.2.2 Recommendations

1. The company's senior management (CEO and Board President) should issue a signed policy statement affirming the company's commitment to the VPSHR and their intention to implement a vigorous and aggressive program to embed the values into all of the company's activities. The company can do this through a public Charter of Principles or similar executive-level policy document. This step communicates to all employees, stakeholders, constituents and contractors that the company will use the VPSHR as a core value of the company and a basis for a strong ethical

and socially responsible business culture. This policy statement should be clear, unambiguous and firm. It represents the personal commitment of company's senior management.

2. While the CEO is responsible for the company's implementation of the VPSHR, a corporate champion (or program manager) is essential to manage the day-to-day actions, steward the process and report progress to the Board and the CEO. The champion is the individual who interacts at the corporate level on behalf of the entire organization. That position may include additional responsibilities (see case study example below).
3. The most rapid and effective way to incorporate the VPSHR into the company's activities is by making implementation a key job responsibility in the performance plan for each operational manager at organization, activity, site and functional level. As a performance objective of all managers, the VPSHR will become a concern rather than a distraction. Defining accountability will assure active support and put wheels under the program.
4. Once the company designates a VPSHR program champion, it will have to provide the budget and the necessary resources to fulfill the responsibilities of the position. This is more than just money. It means recruiting outside expertise, contracting for subject matter experts to conduct training at various levels and building the appropriate staff structure.[1] Until there are dedicated resources, the implementation process will be hostage to the priorities of other departments and risks becoming a façade without substance.

6.3 PHASE TWO: CONSOLIDATING THE INITIATIVE

The VPSHR process will take time to show substance. Announcements and policy statements set the stage for the real work of building the program, establishing the procedures, drafting protocols and adjusting and supervising contracts to reflect the new paradigm.

Scenario 13: Integrated Social Strategy

Without an integrated approach, the company will find an effective implementation of the VPSHR is difficult to impossible. An all too common weakness of corporate social strategies is lack of cohesion. Splitting responsibilities among various departments and supervisors dilutes the effort and destroys synergy. Often the various programs lack coordination, compete for resources and produce overlapping activities. This is wasteful and frequently counter-productive.

One effective corporate project organization combined almost all elements into an Integrated Social Strategy (ISS) under a senior vice president. This centralized planning and resource management. The vice president supervised all programs related to social development, environmental mitigation, public health, government and public relations, media activities, community development and community related security matters worked in tandem toward a common goal. The VP for ISS was the steward, the champion, of the VPSHR implementation process.

This was a large organization with a large span of control. It needed a strong and capable leader. Properly led, it brought together elements that were scattered across several functional staffs and had them working in concert.

For Discussion
How does your company create an integrated approach appropriate to its size and organizational structure?

1 One essential resource is a Business Security Management Plan that will provide the long-term strategic guidance for the security function across the range of its responsibilities, including, but by no means limited to, the VPSHR.

6.3.1 Discussion

The consolidation phase of an effective VPSHR program is the most critical because it is the most substantive. In Phase Two, the company will be able to establish a functioning program that should begin to show action and results. Management will understand their responsibilities to make the VPSHR a vital part of the corporation's activities. The educational, training and outreach efforts will be visible and delivering measurable output. Other security initiatives such as the Community Security Forum will mature, likely changing to adapt to local circumstances. By the second year, corporate management should be able to see many of the indicators of a successful program.

6.3.2 Recommendations

1. Corporate leadership can best support the VPSHR implementation by using the normal course of business meetings with the host government to provide information on the VPSHR and explain the company's commitment to the principles and consequent obligations. This is an educational process by company leaders to members of the host government. The effort, and periodic follow-up sessions, will send the message to all levels of the host government that the company is serious and fully committed to implementing the VPSHR. Doing this meets the expectation inherent in the VPSHR to consult regularly with host governments and to clarify the company's commitment to human rights. These discussions give corporate management the opportunity to raise any allegations of human rights abuses with the host government; this is an expectation of the VPSHR. Planting the VPSHR message at the top has a trickle down effect of accountability within the host government bureaucracy. At each descending level, the subordinates will be aware that the company management regularly meets with their supervisor, that they discuss human rights abuse allegations, and that they protect their own interests by prompt and effective investigation of any suspicious incidents. No bureaucrat wants to explain why he did not fully inform his senior about a delicate issue that surprised that supervisor in a meeting with a major international investor.
2. In Phase Two, the company will have the opportunity to mobilize the resources to build and sustain the VPSHR implementation effort. This effort will often require external expertise, training, workshops and support materials. In Phase Two, the company can procure and make available the posters, representational items and other equipment as needed. This is also the time to contract with an external monitor and schedule the external verification and validation program.
3. During this period, the corporate champion should be able to draft and get the appropriate signatures on the required plans, procedure, processes and protocols needed to support and deliver the VPSHR. These would include a formal process for reporting allegations of human rights abuse, announced and put in place. By this time, the company should have completed and ratified protocols with the police, military, and possibly others. This process includes the company's consultation and clarification of the protocols with the other stakeholders. The training plan for the private security guard service will be refined and underway. The Stakeholder Engagement Plan should have been refined, coordinated within the company and fielded. In short, the company should have evaluated and either accepted, modified or rejected the recommendations identified in Sections II, III, IV and V. Those recommendations that are accepted should be well underway.

Collectively, the measures taken in Phases One and Two are the proof of purchase. When these initiatives are operational and the company has communicated the results to the various stakeholders, the company has conclusively demonstrated a good-faith effort to implement the VPSHR. The payoff, however, is in Phase Three.

6.4 PHASE THREE: LANDING THE VPSHR

In Phase Three, the VPSHR will move from a special focus effort to a core value of the corporation. The VPSHR will be a part of the company's culture, the standard way the company does business. The company and other stakeholders should be able to see the value of the VPSHR by measurable improvement in the process of incident management. Ideally, implementing the VPSHR will have

spurred the professionalism of the public security forces, built confidence in the community, enhanced the pride and behavior of the company workforce and gained the respect of responsible NGOs. The VPSHR are an essential component of a shared responsibility for the overall security of the company's operations and the community.

6.4.1 Discussion

It would be a serious error to assume the VPSHR and the supporting programs will be "completed" in 18 months or less. At best, Phases One and Two will lay the foundations for a security and human rights program that can be effective in protecting the people, property, business continuity and reputation of the company. The rollout of a program, no matter how detailed, will require adjustment and modification as social forces interact with it. Phase Three is the period when the company demonstrates it means what it says.

1. Corporate management, from CEO and board members through the VPSHR champion to the country, site and function managers, should now lead by example. Just as each member of the management team should see themselves as safety officers, so they should also personally identify with the VPSHR and the core corporate values that result from the implementation process. Management can make this happen by personal involvement and commitment. If the VPSHR are to be a sustainable program, it should start at the top with a continuing commitment. Otherwise the VPSHR will simply be another boutique issue, fashionable for a time and then forgotten.
2. In Phase Three, the company should be able to communicate the VPSHR are the company standard of behavior. Any manager should be able to ask any employee, "What do you do if you witness or hear of a human rights incident?" That employee should know the answer because he has been briefed on the procedure, reminded of it, seen posters describing it and possibly has heard of others who have experienced it. The employee will understand its relevance to him and his family and community. Getting to this point will take a very significant effort, but it is essential.
3. The best way to sustain momentum in implementing the VPSHR is to establish performance metrics to measure progress through surveys, questionnaires and external assessments. The independent, external monitor will be a valuable tool in determining the progress of the security and human rights programs. The best metric is to analyze the company's handling of a human rights allegation or serious incident. Unfortunately, the statistical probability is that over time most companies will face serious incidents, at least some involving a risk to life or business viability at that location. How the company manages these incidents will be the true validation of its VPSHR program.
4. The final element of an effective implementation process is the reporting procedure for internal analysis and external transparency. An effective reporting system passes allegations rapidly and directly up the corporate ladder. The follow-on reporting provides context and supporting information. This added detail is used to determine what further actions are required and at what levels. If the allegation is credible, this will definitely mean communicating with the host government and perhaps other select organizations. In all cases, the company needs a procedure to record allegations, internal inquiries and official investigations (if any). In some cases, the company can release the information to other stakeholders. In other cases, the company will only be able to say that it has received and taken appropriate action on all human rights allegations as called for in the VPSHR. The company should not answer questions with an equivocation or a "no comment", both of which are counter-productive. There is no requirement to embarrass or defame the government or public security forces. The company's conversations with the host government may remain confidential and, in most cases, company efforts are more effective if they are handled discreetly.

Voluntary Principles on Security and Human Rights

INTRODUCTION

Governments of the United States, the United Kingdom, the Netherlands and Norway, companies in the extractive and energy sectors ("Companies"), and non-governmental organizations ("NGOs"), all with an interest in human rights and corporate social responsibility, have engaged in a dialogue on security and human rights.

The participants recognize the importance of the promotion and protection of human rights throughout the world and the constructive role business and civil society ?including non-governmental organizations, labor/trade unions, and local communities ?can play in advancing these goals. Through this dialogue, the participants have developed the following set of voluntary principles to guide Companies in maintaining the safety and security of their operations within an operating framework that ensures respect for human rights and fundamental freedoms. Mindful of these goals, the participants agree to the importance of continuing this dialogue and keeping under review these principles to ensure their continuing relevance and efficacy.

Acknowledging that security is a fundamental need, shared by individuals, communities, businesses, and governments alike, and acknowledging the difficult security issues faced by Companies operating globally, we recognize that security and respect for human rights can and should be consistent;

Understanding that governments have the primary responsibility to promote and protect human rights and that all parties to a conflict are obliged to observe applicable international humanitarian law, we recognize that we share the common goal of promoting respect for human rights, particularly those set forth in the Universal Declaration of Human Rights, and international humanitarian law;

Emphasizing the importance of safeguarding the integrity of company personnel and property, Companies recognize a commitment to act in a manner consistent with the laws of the countries within which they are present, to be mindful of the highest applicable international standards, and to promote the observance of applicable international law enforcement principles (e.g., 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), particularly with regard to the use of force;

Taking note of the effect that Companies' activities may have on local communities, we recognize the value of engaging with civil society and host and home governments to contribute to the welfare of the local community while mitigating any potential for conflict where possible;

Understanding that useful, credible information is a vital component of security and human rights, we recognize the importance of sharing and understanding our respective experiences regarding, *inter alia*, best security practices and procedures, country human rights situations, and public and private security, subject to confidentiality constraints;

Acknowledging that home governments and multilateral institutions may, on occasion, assist host governments with security sector reform, developing institutional capacities and strengthening the rule of law, we recognize the important role Companies and civil society can play in supporting these efforts;

We hereby express our support for the following voluntary principles regarding security and human rights in the extractive sector, which fall into three categories, risk assessment, relations with public security, and relations with private security:

RISK ASSESSMENT

The ability to assess accurately risks present in a Company's operating environment is critical to the security of personnel, local communities and assets; the success of the Company's short- and long-term operations; and to the promotion and protection of human rights. In some circumstances, this is relatively simple; in others, it is important to obtain extensive background information from different sources; monitoring and adapting to changing, complex political, economic, law enforcement, military and social situations; and maintaining productive relations with local communities and government officials.

The quality of complicated risk assessments is largely dependent on the assembling of regularly updated, credible information from a broad range of perspectives " local and national governments, security firms, other companies, home governments, multilateral institutions, and civil society knowledgeable about local conditions. This information may be most effective when shared to the fullest extent possible (bearing in mind confidentiality considerations) between Companies, concerned civil society, and governments.

Bearing in mind these general principles, we recognize that accurate, effective risk assessments should consider the following factors:

Identification of security risks. Security risks can result from political, economic, civil or social factors. Moreover, certain personnel and assets may be at greater risk than others. Identification of security risks allows a Company to take measures to minimize risk and to assess whether Company actions may heighten risk.

Potential for violence. Depending on the environment, violence can be widespread or limited to particular regions, and it can develop with little or no warning. Civil society, home and host government representatives, and other sources should be consulted to identify risks presented by the potential for violence. Risk assessments should examine patterns of violence in areas of Company operations for educational, predictive, and preventative purposes.

Human rights records. Risk assessments should consider the available human rights records of public security forces, paramilitaries, local and national law enforcement, as well as the reputation of private security. Awareness of past abuses and allegations can help Companies to avoid recurrences as well as to promote accountability. Also, identification of the capability of the above entities to respond to situations of violence in a lawful manner (i.e., consistent with applicable international standards) allows Companies to develop appropriate measures in operating environments.

Rule of law. Risk assessments should consider the local prosecuting authority and judiciary's capacity to hold accountable those responsible for human-rights abuses and for those responsible for violations of international humanitarian law in a manner that respects the rights of the accused.

Conflict analysis. Identification of and understanding the root causes and nature of local conflicts, as well as the level of adherence to human rights and international humanitarian law standards by key actors, can be instructive for the development of strategies for managing relations between the Company, local communities, Company employees and their unions, and host governments. Risk assessments should also consider the potential for future conflicts.

Equipment transfers. Where Companies provide equipment (including lethal and non-lethal equipment) to public or private security, they should consider the risk of such transfers, any relevant export licensing requirements, and the feasibility of measures to mitigate foreseeable negative consequences, including adequate controls to prevent misappropriation or diversion of equipment which may lead to human rights abuses. In making risk assessments, companies should consider any relevant past incidents involving previous equipment transfers.

INTERACTIONS BETWEEN COMPANIES AND PUBLIC SECURITY

Although governments have the primary role of maintaining law and order, security and respect for human rights, Companies have an interest in ensuring that actions taken by governments, particularly the actions of public security providers, are consistent with the protection and promotion of human rights. In cases where there is a need to supplement security provided by host governments, Companies may be required or expected to contribute to, or otherwise reimburse, the costs of protecting Company facilities and personnel borne by public security. While public security is expected to act in a manner consistent with local and national laws as well as with human rights standards and international humanitarian law, within this context abuses may nevertheless occur.

In an effort to reduce the risk of such abuses and to promote respect for human rights generally, we have identified the following voluntary principles to document relationships between Companies and public security regarding security provided to Companies:

Security Arrangements

Companies should consult regularly with host governments and local communities about the impact of their security arrangements on those communities.

Companies should communicate their policies regarding ethical conduct and human rights to public security providers, and express their desire that security be provided in a manner consistent with those policies by personnel with adequate and effective training.

Companies should encourage host governments to permit making security arrangements transparent and accessible to the public, subject to any overriding safety and security concerns.

Deployment and Conduct

The primary role of public security should be to maintain the rule of law, including safeguarding human rights and deterring acts that threaten Company personnel and facilities. The type and number of public security forces deployed should be competent, appropriate and proportional to the threat.

Equipment imports and exports should comply with all applicable law and regulations. Companies that provide equipment to public security should take all appropriate and lawful measures to mitigate any foreseeable negative consequences, including human rights abuses and violations of international humanitarian law.

Companies should use their influence to promote the following principles with public security: (a) individuals credibly implicated in human-rights abuses should not provide security services for Companies; (b) force should be used only when strictly necessary and to an extent proportional to the threat; and (c) the rights of individuals should not be violated while exercising the right to exercise freedom of association and peaceful assembly, the right to engage in collective bargaining, or other related rights of Company employees as recognized by the Universal Declaration of Human Rights and the ILO Declaration on Fundamental Principles and Rights at Work.

In cases where physical force is used by public security, such incidents should be reported to the appropriate authorities and to the Company. Where force is used, medical aid should be provided to injured persons, including to offenders.

Consultation and Advice

Companies should hold structured meetings with public security on a regular basis to discuss security, human rights and related work-place safety issues. Companies should also consult regularly with other Companies, host and home governments, and civil society to discuss security and human rights. Where Companies operating in the same region have common concerns, they should consider collectively raising those concerns with the host and home governments.

In their consultations with host governments, Companies should take all appropriate measures to promote observance of applicable international law enforcement principles, particularly those reflected in the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms.

Companies should support efforts by governments, civil society and multilateral institutions to provide human rights training and education for public security as well as their efforts to strengthen state institutions to ensure accountability and respect for human rights.

Responses to Human Rights Abuses

Companies should record and report any credible allegations of human rights abuses by public security in their areas of operation to appropriate host government authorities. Where appropriate, Companies should urge investigation and that action be taken to prevent any recurrence.

Companies should actively monitor the status of investigations and press for their proper resolution.

Companies should, to the extent reasonable, monitor the use of equipment provided by the Company and to investigate properly situations in which such equipment is used in an inappropriate manner.

Every effort should be made to ensure that information used as the basis for allegations of human rights abuses is credible and based on reliable evidence. The security and safety of sources should be protected. Additional or more accurate information that may alter previous allegations should be made available as appropriate to concerned parties.

INTERACTIONS BETWEEN COMPANIES AND PRIVATE SECURITY

Where host governments are unable or unwilling to provide adequate security to protect a Company's personnel or assets, it may be necessary to engage private security providers as a complement to public security. In this context, private security may have to coordinate with state forces, (law enforcement, in particular) to carry weapons and to consider the defensive local use of force. Given the risks associated with such activities, we recognize the following voluntary principles to document private security conduct:

Private security should observe the policies of the contracting Company regarding ethical conduct and human rights; the law and professional standards of the country in which they operate; emerging best practices developed by industry, civil society, and governments; and promote the observance of international humanitarian law.

Private security should maintain high levels of technical and professional proficiency, particularly with regard to the local use of force and firearms.

Private security should act in a lawful manner. They should exercise restraint and caution in a manner consistent with applicable international guidelines regarding the local use of force, including the UN Principles on the Use of Force and Firearms by Law Enforcement Officials and the UN Code of Conduct for Law Enforcement Officials, as well as with emerging best practices developed by Companies, civil society, and governments.

Private security should have policies regarding appropriate conduct and the local use of force (e.g., rules of engagement). Practice under these policies should be capable of being monitored by Companies or, where appropriate, by independent third parties. Such monitoring should encompass detailed investigations into allegations of abusive or unlawful acts; the availability of disciplinary measures sufficient to prevent and deter; and procedures for reporting allegations to relevant local law enforcement authorities when appropriate.

All allegations of human rights abuses by private security should be recorded. Credible allegations should be properly investigated. In those cases where allegations against private security providers are forwarded to the relevant law enforcement authorities, Companies should actively monitor the status of investigations and press for their proper resolution.

Consistent with their function, private security should provide preventative and defensive services and should not engage in activities exclusively the responsibility of state military or law enforcement authorities. Companies should designate services, technology and equipment capable of offensive and defensive purposes as being for defensive use.

Private security should (a) not employ individuals credibly implicated in human rights abuses to provide security services; (b) use force only when strictly necessary and to an extent proportional to the threat; and (c) not violate the rights of individuals while exercising the right to exercise freedom of association and peaceful assembly, to engage in collective bargaining, or other related rights of Company employees as recognized by the Universal Declaration of Human Rights and the ILO Declaration on Fundamental Principles and Rights at Work.

In cases where physical force is used, private security should properly investigate and report the incident to the Company. Private security should refer the matter to local authorities and/or take disciplinary action where appropriate. Where force is used, medical aid should be provided to injured persons, including to offenders.

Private security should maintain the confidentiality of information obtained as a result of its position as security provider, except where to do so would jeopardize the principles contained herein.

To minimize the risk that private security exceed their authority as providers of security, and to promote respect for human rights generally, we have developed the following additional voluntary principles and guidelines:

Where appropriate, Companies should include the principles outlined above as contractual provisions in agreements with private security providers and ensure that private security personnel are adequately trained to respect the rights of employees and the local community. To the extent practicable, agreements between Companies and private security should require investigation of unlawful or abusive behavior and appropriate disciplinary action. Agreements should also permit termination of the relationship by Companies where there is credible evidence of unlawful or abusive behavior by private security personnel.

Companies should consult and monitor private security providers to ensure they fulfill their obligation to provide security in a manner consistent with the principles outlined above. Where appropriate, Companies should seek to employ private security providers that are representative of the local population.

Companies should review the background of private security they intend to employ, particularly with regard to the use of excessive force. Such reviews should include an assessment of previous services provided to the host government and whether these services raise concern about the private security firm's dual role as a private security provider and government contractor.

Companies should consult with other Companies, home country officials, host country officials, and civil society regarding experiences with private security. Where appropriate and lawful, Companies should facilitate the exchange of information about unlawful activity and abuses committed by private security providers.

Links and References

Principles and Standards

- Voluntary Principles on Security and Human Rights website – includes the Principles, information on participants and links to participant websites etc.
  www.voluntaryprinciples.org/
- IFC/MIGA Social and Environmental Performance Standards – Performance Standard 4 (PS 4) on Community, Health, Safety and Security includes requirements similar to the voluntary principles.
  www.miga.org/policies/index_sv.cfm?stid=1652
- Guidance Note for Performance Standard 4 – more detailed information to support implementation of PS 4.
  www.ifc.org/ifcext/enviro.nsf/Content/GuidanceNotes
- Equator Principles – the 50+ commercial banks that are signatories to the Equator Principles apply the IFC/MIGA Social and Environmental Performance Standards to project financing in non-OECD countries.
  www.equator-principles.com/index.html
- United Nations – documents on law enforcement referenced in the Voluntary Principles on Security and Human Rights
- Code of Conduct for Law Enforcement Officials
  www.unhchr.ch/html/menu3/b/h_comp42.htm
- Basic Principles on the Use of Force and Firearms
  www.unhchr.ch/html/menu3/b/h_comp43.htm

Implementation of the VPSHR

- Site-level Security Guidelines for the Tangguh LNG project in Indonesia
  www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/downloads/T/Tangguh_Field_Guidelines_BP_Papaun_Police.pdf
- Implementing the VPSHR – documents from Shell
  http://ipoaonline.org/journal/images/journal_2008_0304.pdf
  www.shell.com/home/content/responsible_energy/working_safely/security_and_human_rights/security_human_rights_02042008.html

Toolkits and Information Sources

- International Alert – UN Global Compact and International Institute for Sustainable Development, Conflict-Sensitive Business Practice: Guidance for Extractive Industries
  www.international-alert.org/our_work/themes/business_1a.php
- International Finance Corporation (IFC) CommDev – a website linking to documents and reports relating to many aspects of community development for the oil, gas and mining sectors. Includes sections on human rights and on conflict.
  www.commdev.org
- International Committee of the Red Cross (ICRC) – Business and international humanitarian law: An introduction to the rights and obligations of business enterprises under international humanitarian law.
  www.icrc.org/Web/Eng/siteeng0.nsf/html/business-ihl-150806

- International Business leaders Forum (IBLF) and IFC – Guide to Human Rights Impact Assessment and Management: Road Testing Draft. An eight-step process for businesses to identify, assess and implement measures to strengthen their company's contribution to human rights protection.
  www.iblf.org/activities/Business_Standards/Human_Rights.jsp

- IPIECA (The International Petroleum Industry Environmental Conservation Association) – Tools to provide practical help for member companies, and a wider industry audience, understand and improve practice on existing and emerging social responsibility issues:
  - Guide to Operating in Areas of Conflict for the Oil & Gas Industry
  - Human Rights Training Toolkit for the Oil and Gas Industry

  www.ipieca.org/activities/social/social_publications.php#5

- US Department of State Country Reports on Human Rights Practices – submitted annually by the U.S. Department of State to the U.S. Congress.
  www.state.gov/g/drl/rls/hrrpt/

Business and Human Rights

- In July 2005, Kofi Annan appointed Professor John G. Ruggie to be Special Representative of the UN Secretary-General on business and human rights. The complete list of documents prepared by and submitted to John Ruggie (as of 1 May 2008) can be found at
  www.business-humanrights.org/Gettingstarted/UNSpecialRepresentative

Links active as of 8 May 2008

Extracts

IFC/MIGA PERFORMANCE STANDARD 4

Security Personnel Requirements

13. **When the client directly retains employees or contractors to provide security to safeguard its personnel and property, it will assess risks to those within and outside the project site posed by its security arrangements. In making such arrangements, the client will be guided by the principles of proportionality, good international practices in terms of hiring, rules of conduct, training, equipping and monitoring of such personnel, and applicable law. The client will make reasonable inquiries to satisfy itself that those providing security are not implicated in past abuses, will train them adequately in the use of force (and where applicable, firearms) and appropriate conduct toward workers and the local community, and require them to act within the applicable law. The client will not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat. A grievance mechanism should allow the affected community to express concerns about the security arrangements and acts of security personnel.**

14. **If government security personnel are deployed to provide security services for the client, the client will assess risks arising from such use, communicate its intent that the security personnel act in a manner consistent with paragraph 13 above, and encourage the relevant public authorities to disclose the security arrangements for the client's facilities to the public, subject to overriding security concerns.**

15. **The client will investigate any credible allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to public authorities when appropriate.**

GUIDANCE NOTE ON IMPLEMENTATION

G27. Security arrangements to protect a client's personnel and property will typically depend in large part on security risks in the operating environment, though other factors, such as company policy or the need to protect intellectual property or hygiene in production operations, can also influence security decisions. In determining what security arrangements and equipment are necessary, clients should apply the principle of proportionality. In many circumstances, a night watchman may be all that is required, together with some basic security awareness training for staff, sign-posting, or well-placed lighting and fences. In more complex security environments, the client may have to directly employ further security personnel or engage private security contractors or even work directly with public security forces.

G28. It is important for clients to assess and understand the risks involved in their operations, based on reliable and regularly updated information. For clients with small operations in stable settings, a review of the operating environment can be relatively straightforward. For larger operations or those in unstable environments, the review will be a more complex and thorough risk assessment that may need to consider political, economic, legal, military and social developments, and any patterns and causes of violence and potential for future conflicts. It may be necessary for clients to also assess the record and capacity of law enforcement and judicial authorities to respond

appropriately and lawfully to violent situations. If there is social unrest or conflict in the project's area of influence, the client should understand not only the risks posed to its operations and personnel but also whether its operations could create or exacerbate conflict. Conversely, if provided consistent with Performance Standard 4, the client's operations involving the use of security personnel may avoid or mitigate adverse impacts on the situation and contribute to the improvement of security conditions around the project area. Clients should consider security risks associated with the entire range and stages of their operational activities, including personnel, products and materials being transported. The assessment should also address negative impacts on workers and the surrounding communities, such as the potential for increased communal tensions due to the presence of security personnel or the risk of theft and circulation of firearms used by security personnel.

G29. Community engagement is an important aspect of an appropriate security strategy, as good relations with workers and communities can be the most important guarantee of security. Clients should communicate their security arrangements to workers and the affected community, subject to overriding safety and security needs, and involve workers and surrounding communities in discussions about the security arrangements through the community engagement process described in Performance Standard 1.

G30. Clients should require the appropriate conduct of security personnel it employs or engages. Security personnel should have clear instructions on the objectives of their work and permissible actions. The level of detail of the instructions will depend on the scope of permitted actions (particularly if security personnel are permitted to use force and in exceptional circumstances, firearms) and the number of personnel. The instructions should be based on applicable law and professional standards. These instructions should be communicated as terms of employment and reinforced through periodic professional training.

G31. If security personnel are permitted to use force, instructions must be clear on when and how force may be used, specifying that security personnel are permitted to use force only as a matter of last resort and only for preventive and defensive purposes in proportion to the nature and extent of the threat, and in a manner that respect human rights (see paragraph G26 below). When the use of firearms is appropriate, any firearms and ammunition issued should be licensed, recorded, stored securely, marked and disposed of appropriately. Security personnel should be instructed to exercise restraint and caution, clearly prioritizing prevention of injuries or fatalities and peaceful resolution of disputes. Use of physical force should be reported to and investigated by the client. Any injured persons should be transported to medical facilities.

G32. The appropriate conduct of security personnel should be based on the principle that providing security and respecting human rights can and should be consistent. For example, any security personnel who interact with workers should not harass or intimidate workers exercising their rights in accordance with Performance Standard 2. If community members decide to associate, assemble and speak out in opposition to the project, the client and any security personnel who interact with them should respect the right of the local communities to do so. The instructions for security personnel should also make clear that arbitrary or abusive use of force is prohibited.

G33. Who provides security is as relevant as how security is provided. When employing or engaging any security personnel, the client should make reasonable inquiries to investigate the employment record and other available records, including any criminal record, of individuals or firms and should not employ or use any individuals or companies that have been credibly alleged to have abused or violated human rights in the past. Clients should use only security professionals who are and continue to be adequately trained.

G34. The client should record and investigate security incidents to identify any necessary corrective or preventive actions for continuing security operations. To promote accountability, the client (or other appropriate party such as the security contractor or appropriate public or military authority) should take corrective and/or disciplinary action to prevent or avoid a repetition if the incident was not handled according to instructions. Unlawful acts of any security personnel (whether employees, contractors or public security forces) should be reported to the appropriate authorities (bearing in mind that clients may have to use their judgment about reporting violations if they have legitimate concerns about treatment of persons in custody). Clients should follow-up on reported unlawful acts by actively monitoring the status of investigations and pressing for their proper resolution. The grievance mechanism required under Performance Standard 1 provides another avenue for workers or community members to address concerns about security activities or personnel within the client's control or influence.

G35. There may be cases where the government decides to deploy public security forces to protect a client's operations, whether on a routine or as needed basis. In countries where it is illegal for companies to employ private security forces, the client may have no choice but to engage public security forces to protect its assets and employees. Governments have the primary responsibility for maintaining law and order and the decision-making authority with respect to deployments. Nonetheless, clients whose assets are being protected by public security forces have an interest in encouraging those forces to behave consistently with the requirements and principles set out above for private security personnel in order to promote and maintain good relations with the community, bearing in mind that public security forces may be unwilling to accept restrictions on their ability to use offensive force where they consider necessary. Clients are expected to communicate their principles of conduct to the public security forces, and express their desire that security be provided in a manner consistent with those standards by personnel with adequate and effective training. The client should request that the government make information about the arrangements to the client and the community, subject to overriding safety and security needs. If clients are required or requested to compensate the public security forces or provide equipment to public security forces, and if the option of declining the request is not available or desirable, clients may choose to provide in kind compensation, such as food, uniform, or vehicles, rather than cash or lethal weapons. Clients should also try to implement restrictions, controls and monitoring as necessary and possible under the circumstances to prevent misappropriation or use of the equipment in a manner that is not consistent with the principles and requirements set out above.

G36. Pursuant to the requirement of paragraph 15 of Performance Standard 4 to report unlawful and abusive actions to public authorities, IFC may require its client to update IFC on the client's use of security personnel and any material developments and incidents as part of periodic monitoring reports to be submitted to IFC."

Source: Extracted from *www.miga.org/policies/index_sv.cfm?stid=1589* Text in bold is from PS4; light-face text is from the Guidance Note on Implementation of PS4.

Voluntary Principles Implementation Tracking

Effective Programs	RED: INSUFFICENT YELLOW: MORE WORK NEEDED GREEN: IN PLACE

PRINCIPLES	FOCUS AREAS	STATUS AS OF [*DATE*]		
		LOCAL	NATIONAL	CORPORATE
RISK ASSESSMENT	Processes: • for regular risk assessment • for acting on findings			
	Mechanisms for regular consultation with communities about the impact of Company security arrangements on community members : • project affected villagers • artisanal miners • local leaders Incorporation of community concerns in site level plans			
	Scope of Risk Assessment includes:			
	Identification of Risks:			
	Potential for Violence • between community and company • between community and government			
	Human Rights Records			
	Rule of Law			
	Conflict Analysis			
RISK ASSESSMENT (cont.)	Equipment Transfers			
	What organizations of public security are involved:			
	Security Arrangements			

PRINCIPLES	FOCUS AREAS	STATUS AS OF [*DATE*]		
		LOCAL	NATIONAL	CORPORATE
	Deployment and Conduct			
	Consultation and Advice			
	Responses to Human Rights Abuses			
RELATIONS WITH PRIVATE SECURITY	Involvement of private security contractors (PSC)			
	Policies regarding ethical conduct			
	Level of technical and professional proficiency			
	Act in lawful manner			
	Policies on appropriate conduct and use of force			
	Record of allegations of Human rights abuse			
	Provide preventative and defensive services			
	Employment policies of private security contractor			
	Properly investigate and report incidents			
	Maintain confidentiality of information			
	Voluntary principles outlines as contractual provision			
	Consult and Monitor private security providers			
	Review background of private security			
RELATIONS WITH PRIVATE SECURITY (cont.)	Consult with other companies			
INTEGRATION OF VPSHR INTO MANAGEMENT SYSTEM	Corporate Commitment			
	Policy			

PRINCIPLES	FOCUS AREAS	STATUS AS OF [*DATE*]		
		LOCAL	NATIONAL	CORPORATE
	Defined responsibilities and accountabilities			
	Interface between community relations and security			
	Resources: people/budget etc			
	Standards, protocols, integration into security management plans/SOPs etc			
	Training			
	Performance measurement; team building			
	Security policy and program review process			
	Reporting: • **internal** • **external**			
	Internal communication of goals, expectations and standards			

World Bank Group
Multilateral Investment Guarantee Agency
1818 H Street, NW
Washington, DC 20433
USA

www.miga.org