Good Practice Note

Environment & Social Framework for IPF Operations

Assessing and Managing the Risks and Impacts of the Use of Security Personnel

THE WORLD BANK
IBRD • IDA

First Edition
Published October 2018

This Good Practice Note was prepared by Charles di Leva, Afshan Khawaja, Anne-Katrin Arnold, and Elizabeth Temple Smith. It is informed by the Good Practice Handbook on Use of Security Forces: Assessing and Managing Risks and Impacts published by the International Financial Corporation (IFC).

Abbreviations

ESCP	Environmental and Social Commitment Plan
ESF	Environmental and Social Framework
ESMP	Environmental and Social Management Plan
ESMS	Environmental and Social Management System
ESRS	Environmental and Social Review Summary
ESS	Environmental and Social Standard
FCV	Fragility, conflict and violence
FI	Financial intermediary
GPN	Good Practice Note
IFC	International Finance Corporation
IPF	Investment Project Finance
ISR	Project Implementation Status and Report
MoU	Memorandum of Understanding
NGO	Nongovernmental organization
SEP	Stakeholder Engagement Plan
SMP	Security Management Plan
SRA	Security Risk Assessment
UN	United Nations

Contents

1. Introduction

Environmental and Social Framework

The World Bank's Environmental and Social Framework (ESF) requires that Borrowers assess and manage potential environmental and social risks and impacts arising from projects that the World Bank supports through Investment Project Financing (IPF). These risks and impacts are described in the Environmental and Social Policy (paragraph 4) as well as in Environmental and Social Standard 1 (Assessment and Management of Environmental and Social Risks and Impacts, paragraph 28) and related provisions. They include, among others, threats to human security through personal, communal or interstate conflict, crime or violence.

Potential threats to project workers, sites, assets and activities as well as to project-affected communities are assessed and mitigated by the Borrower throughout the project life cycle. If it is decided that security personnel should be engaged, the potential risks and impacts stemming from such engagement in turn needs to be assessed and management measures identified in accordance with the mitigation hierarchy.

Security personnel can be private (employees of a private security company) or public (such as police or military personnel). They can be engaged by the project contractor, or by the Borrower. Their presence can pose risks to, and have unintended impacts on, both project workers and local communities. For example, the way in which security personnel interact with communities and project workers may appear threatening to them or may lead to conflict. A clear Code of Conduct for the project's workers, including security personnel, can help to mitigate this risk by specifying what constitutes unacceptable behavior. Separately, a binding agreement with security personnel will require, among other matters, that use of force always be proportional to the nature of the incident.

Box 1: World Bank's Good Practice Notes

The World Bank is providing a series of Good Practice Notes (GPN) to accompany the ESF to support its implementation. The GPN have been developed in partnership with specialists from inside and outside the Bank and are designed to be reviewed and updated periodically, when appropriate. This Note focuses on assessing and managing the risks of the use of security personnel in IPF. It should be read in conjunction with the ESF, including the Policy, the Environmental and Social Standards (ESS1-10) and the accompanying Guidance Notes for Borrowers.

This GPN (see Box 1) is intended to support project teams and environmental and social specialists as they work with Borrowers in assessing and managing risks to the human security of project-affected communities and project workers that could arise from the use or presence of security personnel that have been engaged to protect the project or related aspects.

Roles and Responsibilities

The Borrower is responsible for the assessment of security risks for the project, including security risks to project workers, assets, and activities. This Security Risk Assessment (SRA) is typically part of the environmental and social impact assessment (ESIA) and includes a determination of the level of security required for the project. Where such risks are considered low, security arrangements might consist of simple measures, such as fencing or signs and security guards at night. Where security risks are considered more substantial, the Borrower and/or contractors might choose to engage private security providers or work with public security personnel to provide protection. In high-risk situations, particularly in situations of fragility, conflict and violence (FCV), the Borrower is more likely to choose to deploy public security forces.

Once the Borrower and/or contractor have determined that security personnel should be engaged to protect project workers, sites, assets or activities, the Borrower assesses risks to and impacts on human security that could arise from the engagement of such personnel. The scale and scope of the SRA will vary greatly, based on the project context.

Depending on the severity and complexity of the security risk, the Borrower should prepare a stand-alone Security Management Plan (SMP) and/or ensure that key elements of the security assessment and arrangements are reflected in the Environmental and Social Commitment Plan (ESCP) for the Project. This includes mitigation measures to manage risks to the human security of project-affected communities and project workers that could arise from the use of security personnel. Mitigation measures that have security benefits or reduce security impacts may be closely linked to social investment or other social mitigation measures.

The Bank should support the Borrower in understanding the relevant requirements of the ESF, including those related to risks to and impacts on human security, so that it can complete the assessments and management plans to the satisfaction of the Bank, and implement the project as agreed. For projects that engage security personnel, the Bank's environmental and social specialists should work closely with operational procurement staff. Discussions with the Bank's Corporate Security Specialists may also be necessary, especially where there are risks to Bank staff or consultants in traveling to or engaging in activities at the project site.

Where required, particularly due to weak Borrower capacity, the Bank may help the Borrower determine the scale and extent of the security risk assessment, depending on the needs and potential risks and impacts of the project. The Borrower's assessment should demonstrate that it has identified and evaluated relevant security risks and has consulted project stakeholders, including project-affected communities, local nongovernmental organizations (NGOs), local businesses and other groups that may be particularly aware of security issues**.** The Borrower may require external assistance in undertaking this process. To avoid a conflict of interest, as a general rule, external firms that are used to carry out the SRA should not be eligible for further risk management activities on the particular project.

Bank project teams should have an initial understanding of a project's security risks, in regard to the type of project, its location, and the political context in the country. Key sources of information on an investment project's social and political context, security-related risks, and potential risks posed by use of security personnel include:

- Bank Country Offices, especially in higher-threat locations, which often have resident Security Specialists who can provide general security information on the country.[1]
- The Bank's Corporate Security Department, which provides security risk assessments.[2] Corporate Security also has a team of regionally focused Security Risk Analysts who can provide additional security guidance.
- Experience from previous Bank-funded projects or those of other financiers or donors.

[1] Available at https://gsdapps.worldbank.org/traveladvisory/ in each country's contacts section, or via email inquiries to WBGSecurity@worldbank.org. This and other links in this document may only be available internally to Bank staff and consultants.

[2] Available at http://workgroup.worldbank.org/org/units/GSD/GSDCS/Pages/Security-Risk-Management-ver-1.aspx

- Advisory information from UN agencies and international and local NGOs.
- Annual indices and reports on country-level indictors of conflict, human rights issues, etc.
- Media articles and reports.
- Specific industry and location (at regional and community level) information.
- Proposed contractor(s) information.

2. Assessing the risks and impacts of the use of security personnel

The need to address the assessment and mitigation of risks to, and impacts from, the use of security personnel on project-affected communities and project workers is set out in various Environmental and Social Standards (ESSs). These are shown in Table 1:

Table 1. Human Security and the Environmental & Social Standards

ESS1. Assessment and Management of Environmental and Social Risks and Impacts

ESS1 addresses the need to assess environmental and social assessment risks and impacts, including those related to human security.

> *"Annex 1 5(e) Social and conflict analysis is an instrument that assesses the degree to which the project may (a) exacerbate existing tensions and inequality within society (both within the communities affected by the project and between these communities and others); (b) have a negative effect on stability and human security; (c) be negatively affected by existing tensions, conflict and instability, particularly in circumstances of war, insurrection and civil unrest."*

ESS4. Community Health and Safety

ESS4 addresses the health, safety, and security risks to and impacts on project-affected communities and the corresponding responsibility of Borrowers to avoid or minimize such risks and impacts, with particular attention to people who, because of their particular circumstances, may be vulnerable.

> *"24. When the Borrower retains direct or contracted workers to provide security to safeguard its personnel and property, it will assess risks posed by these security arrangements to those within and outside the project site. In making such arrangements, the Borrower will be guided by the principles of proportionality and GIIP, and by applicable law, in relation to hiring, rules of conduct, training, equipping, and monitoring of such security workers. The Borrower will not sanction any use of force by direct or contracted workers in providing security except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.*
>
> *25. The Borrower will seek to ensure that government security personnel deployed to provide security services act in a manner consistent with paragraph 24 above, and encourage the relevant authorities to disclose the security arrangements for the Borrower's facilities to the public, subject to overriding security concerns.*
>
> *26. The Borrower will (i) make reasonable inquiries to verify that the direct or contracted workers retained by the Borrower to provide security are not implicated in past abuses; (ii) train them adequately (or determine that they are properly trained) in the use of force (and where applicable, firearms), and appropriate conduct toward workers and affected communities; and (iii) require them to act within the applicable law and any requirements set out in the ESCP.*
>
> *27. The Borrower will review all allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence*

> *and, where necessary, report unlawful and abusive acts to the relevant authorities."*

ESS9. Financial Intermediaries

ESS9 addresses the need to ensure that the requirements of the ESSs are understood by the Financial Intermediaries (FIs).

> *"20. The FI will ensure that the requirements of this ESS and ESS2 are clearly communicated to all relevant FI personnel and ensure that relevant personnel have the necessary knowledge and capabilities for managing environmental and social risks in accordance with the FI's [Environmental and Social Management System (ESMS)]."*

In general, when the Borrower determines that it is necessary to incorporate an assessment of security-related risks and impacts in the ESIA, key elements of such assessment should include:

- Country context (e.g., conflict, criminality, governance/rule of law, physical environment, socio-economic situation);
- National/local security issues (e.g., availability of security personnel, track record, including allegations with any link to abuse, and professional reputation of private security and public security personnel);
- Risks from other external threats (e.g., to workforce/contractors at or in transit to remote construction sites);
- Risks to human safety and security of assets perceived by community members, due to the presence of the project (including any private or public security);
- Risks to workers from security personnel, including non-compliance with the Code of Conduct;
- Preliminary recommendations (prioritized) for prevention and mitigation, and agreements needed with security responders to mitigate risks;
- Potential opportunities to employ women in the security personnel for the project;
- An institutional and legal analysis that identifies potentially affected persons and groups, assesses potential impacts, in particular on those that are disadvantaged or vulnerable, and that develops relevant mitigation measures.

The SRA should include an analysis of contextual factors that could cause or exacerbate human security risks. For example, tensions between community members, local businesses, sub-contractors and other stakeholders and security personnel may arise due to actual or perceived project impacts as well as actual or perceived behavior of security personnel. In particular, interactions between communities and security personnel can lead to tensions if the security personnel are involved in enforcing land acquisition and resettlement, protecting extractive industry sites, preventing access to cultural heritage sites, or transporting or disposing of solid or hazardous waste. Communities may feel threatened by security personnel if the project disturbs community lands or project community benefit-sharing arrangements have not been implemented, or if the behavior of the security personnel is perceived to be threatening to their well-being or business activities.

When assessing security risks, it is important to engage with stakeholders, including project-affected communities, local NGOs, and other groups that may be particularly aware of security issues. Box 2 lists indicative questions that could be asked when assessing risks to and impacts on human security stemming from the use of security personnel.

Box 2. Sample questions for Security Risk Assessments

- What is the potential for conflict in and around the project area (for example, escalation of violence based on grievances, regional protests)?
- Are there different project locations, with different risk profiles? Are some project areas higher risk or do they need more security than others?
- Does the nature of the project itself pose any risks to the community?
- Is the presence of security personnel proposed to be temporary or long-lasting?
- Are public security personnel already deployed to the project site? If so, is it possible to see the agreement or memorandum of understanding (MoU) regarding the deployment and to review it for reference to behavior, Code of Conduct and proportional force?
- If security personnel already are in existence at the proposed project site/facilities, who is currently providing security? Are there any historical or legacy issues with these security providers that may still be relevant? How have security incidents been handled, and by whom (for example, by project security personnel or by local police or others)? What kind of vetting was undertaken prior to employment or contracting?
- Does the Borrower have any concerns about the reputation or behavior of private or public security personnel? Have there previously been any incidents concerning security personnel in the country or project region? Is the Borrower able to request or require removal of individuals from the project services if they do not comply with the Code of Conduct or other project requirements?
- Will security personnel be armed? If so, what security risk assessment was done to come to that decision and under what conditions can force be used? Are there guard dogs, barricades, barbed wire, or other defenses? Is the management of weapons and other defenses structured and are procedures clear?
- Are security personnel engaged in accompanying high value assets or transportation of raw or hazardous materials and production? If so, what are the additional and specific arrangements in terms of risk assessment, prevention, mitigation, and response planning?
- Is the project exposed to targeted pressure from local/regional political establishments, NGOs, etc.? What agreements have been made or are expected to be made with regard to the project?
- Do the planned security personnel originate from the project area, or have the same religion/race/ethnic background as local communities and other project workers? Do they speak the same language/dialect? Are there risks of tension due to different backgrounds among the security personnel, community members, and project workers?

Bank project teams should maintain a continuous dialogue with Borrowers about security issues and arrangements where the Borrower or a contractor engages security personnel. It may be advisable for the Borrower to engage independent experts or third parties with specific security expertise to develop security risk assessments and management plans when a project is located in a high-risk area. Examples of such high-risk areas include those in or adjacent to a conflict zone, where there are terrorist activities, or where there is a high prevalence of gender-based violence. The Borrower should appoint a suitable focal point for managing security issues and this individual's role should be reflected in the contract with privately engaged security personnel or in the arrangements for public sector security personnel. The focal point can be an in-house staff member or a consultant; however, to be effective and credible, particularly when interacting with security personnel, the individual should have significant experience with security risk management. A senior project manager should maintain oversight and review all evaluations and recommendations of the SRA to ensure that the assessment and proposed prevention/mitigation measures are reasonable and appropriate to the project and context (particularly if an external firm tasked with the SRA is also bidding for the risk management work).

Given the FCV context in which some projects are located, and often in response to different phases of the project, when risks may be higher or lower, it is important that security risk management and mitigation be adaptive and able to change in response to needs. If security issues escalate or de-escalate, the SRA and any management plans should be adjusted, following discussion with the Bank. A summary of material changes should also be communicated to local stakeholders consistent with stakeholder engagement and information disclosure requirements in ESS10.

3. Mitigating risks and impacts in the use of security personnel

Risks to and potential impacts on human security due to the engagement of security personnel can be mitigated through measures set out in procurement documents and other forms of written agreements, as well as in specific management plans. The Borrower and/or its contractor are responsible for the relevant documentation, and for developing it in consultation with the Bank. The Bank and Borrower agree on whether or not preparation of a stand-alone SMP is required. If security risks are not expected to be significant, their management can be included in the ESCP and/or another relevant document, such as an Environmental and Social Management Plan (ESMP), rather than an SMP.

Some mitigation measures that reduce security risks and impacts may be associated with social programs, such as community investment, or good stakeholder engagement with local communities. It is important that security not be viewed in isolation from the overall social assessment and mitigation process.

Security Management Plans

For projects with high security risks, a stand-alone SMP contains all the procedures and protocols related to security for the project. Building on the SRA, the SMP describes how and by whom security will be managed and delivered, the resources required, and the behavior that is expected of security personnel. It should cover their equipment and responsibilities, as well as the security risks related to security personnel behavior and impacts on communities outlined in ESS4.

While the SMP should be an actionable and practical document, it is unlikely to be able to address every possible scenario in detail. Rather, it should outline the project's general approach to security and define how security is undertaken and how risks are mitigated. The level of effort in managing security risks should be commensurate with the level of security risk associated with the project and its operating context. The SMP document should be in a format that can be audited for compliance purposes. Annex 2 provides a sample outline.

The SMP should include reference to relevant international standards, such as the UN Basic Principles on the Use of Force or the International Code of Conduct for Private Security Providers.

Key commitments in the SMP should be reflected in the ESCP. For projects with low security risk, the commitments are incorporated directly into the ESCP, which notes the major risks related to security and the use of security personnel as well as the measures to be implemented by the Borrower to mitigate those risks.

In reviewing security-related documents such as the SMP, Bank staff should look for the following:

- A requirement for the private company or public agency to have essential due diligence elements in place for vetting security personnel. For example, the company or agency should vet its staff or force to ensure that they are of good character and not associated with a history of abuse. Such abuse includes actions that violate the safety and security of a person or persons (such as deprivation of life/liberty/security, torture, extra-judicial killing, rape or other gender-based violence, including sexual exploitation or abuse).

  Establishment by the company or agency should also include the following:

  - Code of conduct, behavior commitments, clear and accessible disciplinary process, and grievance process;
  - Regular training requirements (specifying the type, frequency, completion rates);

  - For private companies, clear management systems for security/asset protection, and for interactions between it and the Borrower and contractor.

- For situations that might escalate to a point that private project security cannot manage without the support of public security personnel, coordination of security management between authorized public security personnel in high-risk environments, including handover procedures in an escalating situation, any joint training or exercises (including scenario training).
- Engagement with communities about the project's impacts on community safety and security, awareness raising concerning the Code of Conduct commitment and project grievance mechanism, as outlined in the Stakeholder Engagement Plan (SEP) and SMP.
- References to "good international industry practice" (see example of resources in Annex 1).
- Policy on "use of force" and clarity on proportionality to risk. The use of force by direct or contracted workers in providing security should not be sanctioned except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.
- Weapons: if used by security, why, who, what, and how they are controlled (this includes firearms, as well as nonlethal weapons and guard dogs).
- Grievance mechanism(s) for project workers and for the public: clear and transparent process for allegations of abuse to be reported. Special attention to how allegations of gender-based violence are to be managed. Who is to manage grievances related to security whether raised by workers or by the public. Clear prohibitions against any form of retaliation for raising grievances. Protection of confidentiality of the person filing the grievance.
- Incident reporting: means of receiving and reporting incidents and allegations, and guidelines for receiving and following up on them, including procedures for reporting to the Borrower and the Bank, as required.
- Site access control: guidelines for security personnel on how to interact with community members seeking access to a project site or raising a concern (for example, training on the grievance mechanism and Code of Conduct).
- Whether/how the SMP is developed in coordination with other management plans (such as the ESMP or SEP).
- Inclusion of cost estimates for the implementation of the SMP and plans for their review, including after any material changes or incidents. Clarification on whether the budget for the SMP is included in the project budget.
- Information on project interactions with national and international security (for example, UN security forces), as appropriate.

Box 3 includes a checklist for Bank staff due diligence on SMPs.

Box 3. Checklist for Security Management Plans

- Are the findings of the SRA adequately reflected in the Appraisal Environmental and Social Review Summary (ESRS)?
- Has an SMP been prepared? If not, will the SMP be prepared during Project implementation?
- Does the SMP reflect the key issues identified in the SRA, including those related to the project and its context?
- Has a summary or description of the SMP been disclosed to the nearby communities/stakeholders, including reference to the Code of Conduct and project grievance mechanisms for workers and the public?
- Is a third-party security expert needed?
- Are the risk mitigation actions specified in the SRA included in the SMP? Will the Project involve sub-contractors for security?
- Does the ESCP provide for the SMP to be included in bidding documents with contractors?
- Has the budget for the SMP been reviewed by the Bank, and the source of funding identified?

Procurement documents and other forms of written agreements

Specific risk management and mitigation measures may differ depending on whether a contractor engages private security personnel, or whether the Borrower and contractor agree that public security personnel will be used to provide security for the project. In the case of private security companies, Implementing agencies and contractors may have control over the personnel contracted for the project, but monitoring security issues is important, and agencies and contractors should be aware that these issues are being monitored by the Borrower. Although security is often sub-contracted, ultimately, the Borrower is responsible for the commitments made on the project. Contracts should include clear commitments regarding a Code of Conduct; training of proposed private security personnel and vetting of their record, as well as security procedures in case of alleged contract or Code of Conduct violations, including for cases where security personnel use excessive force, intimidation, or retaliation; and a summary of sanctions applicable.

Where public security personnel (e.g., police, military) are provided directly by the Borrower (such as through police or military), the implementing agency and contractor are unlikely to have full control or oversight. A binding memorandum of understanding (MoU) or other formal agreement should be documented, committing the public security force to the project's Code of Conduct, proportional use of force, and other requirements similar to those that would be included in a contract with private security providers, including disciplinary measures, training, incident follow-up and the need for regularly updating of the documentation. The binding agreement should make provisions for establishment of a commission with responsibility for monitoring security conditions and a communication protocol with established spokespersons for the Borrower, the security personnel and the Bank. Such a project-specific agreement is advisable, even when regulations governing public security personnel and their behaviors are in place. The vetting procedures contained in the agreement or MoU with the public security provider should exclude from working related to the project those individuals with a history of past violations or abuse. If the provider does not have vetting procedures, this omission should be viewed as a project risk, and more detailed information may be needed in the MoU or other agreement on the Code of Conduct for the project on how this risk will be avoided, or at least mitigated and managed, and how grievances concerning alleged violations will be handled.

If public security personnel are expected to respond in the case of an incident, or are deployed in or around the project site, Bank staff should confirm that the Borrower has assessed and addressed associated risks. The Borrower should assess the past record of public security personnel, particularly in the communities in the project area, and identify potential risks. The SMP should incorporate reference to the Borrower's MoU or other binding agreement. If public security personnel are involved in the security of the site, the SMP should note the criteria for behavior that must be reflected in the contractor's Code of Conduct, as well as roles and responsibilities of the project team, the contractor and the security force. Security incidents should be documented on an ongoing basis (see section 4 below). Investigations of allegations against security personnel and non-compliance with the Code of Conduct should be undertaken by an experienced and neutral party.

4. Implementation and monitoring

Monitoring project commitments and performance is an important task of Bank staff. Monitoring security commitments and performance is particularly important where 1) the project is designated as High or Substantial for potential risks or impacts related to security, 2) there have been incidents involving security during project implementation, 3) if there are records of grievances involving security or public unrest, or 4) if the security profile of the project has changed for the worse. Annex 3 contains a detailed checklist for planning and implementing site visits to monitor security issues.

Risks related to security and security personnel observed during supervision missions should be noted in the Environmental and Social Review Summary (ESRS). The level of detail in this analysis should be proportional to the level of risk and be referenced in the project Implementation Status and Report (ISR). The ISR should note any significant changes in the security situation and/or the composition of private security and/or provision of public security. These should also be noted in supervision reports on environment and social performance along with a summary of incidents or credible allegations of abuse by public or private security personnel in or around the project site, as well as updates on actions/follow-up related to previous incidents or allegations. The ISR should also include an update on any meetings that have taken place with public security providers on security commitments, performance, grievance management or the Code of Conduct.

For projects with armed security, the ISR should note updates on training on use of force, Code of Conduct, and commitments to meet good international industry practice. It should also take into account the requirements and follow-up on the rotation of personnel.

The SMP should be reviewed during supervision missions by the Bank. Depending on the level of risk, and where appropriate, this review may take place through an independent security audit.

Significant changes in the project's security situation should be reported immediately to the Bank, which will allow for necessary changes to the SMP or ESCP. *Equally,* ***allegations of security personnel non-compliance with the Code of Conduct should be investigated.*** If allegations include gender-based violence an expert in dealing with this issue should be included in the investigation and be responsible for any discussion with survivors. This is true whether the allegations concern project workers or members of the public.

The project-level grievance mechanism that is required by ESS10 should explicitly note its acceptance of grievances related to security and the use of security forces. Project-affected communities should be made aware of the grievance mechanism and the types of issues that can be brought to its attention. Complaints related to security personnel should be logged/registered as is required for any other complaint, and worker and community concerns related to security personnel should be addressed promptly. The Bank should review the grievance logs as part of project supervision and engage with the Borrower as necessary to address issues related to security and the use of security personnel.

Community engagement

In project planning, implementation and supervision, close attention should be paid to stakeholder engagement particularly as it relates to security personnel. Community engagement is a central aspect of a good security program, and good relations with workers and local communities can substantially contribute to overall security in the project area. Having women employed as part of the security team may help reduce tension or incidents involving local communities and should be encouraged. Dialogue with communities about security issues can help to identify potential risks and local concerns, and can serve as an early warning system. Community members should be aware of their ability to make complaints without fear of intimidation or retaliation. Because guards often are the first point of contact with community members at the project gates, they should also be informed about their role in community relations and about the grievance mechanism and key issues of concern to local communities.

Grievances and incidents involving security personnel

As part of project supervision, Bank staff review incident reports submitted to the Bank, and grievance mechanism logs regarding grievances or allegations that involve project-related security personnel. Security-related allegations or incidents can include issues such as theft, abuse of power and retaliation, sexual harassment and exploitation, gender-based violence, and bribery and corruption. Bank staff should request more information about any reported incidents and steps taken to address the issue and prevent recurrence and should promptly keep Bank Management informed of allegations or instances of violence or abuse and the remedial efforts. Allegations or incidents related to security personnel should be documented and assessed with the objective of determining compliance or noncompliance with policies and procedures and whether any corrective or preventive actions are required. Unlawful or abusive acts should be reported to appropriate authorities, including Bank Management, and project management should actively monitor the status of any ongoing criminal investigations and cooperate fully. Project staff responsible for the project SEP and Grievance Mechanism should communicate outcomes to complainants and other relevant parties, keeping in mind confidentiality provisions and the need to protect victims from further incidents or retaliation. Where appropriate, it can also be constructive to share relevant lessons learned with the community and any changes made to prevent future incidents.

Where incidents or grievances regarding security have been identified, the risk profile of the project may need to change, and the Bank's supervision may need to increase, such as more frequent monitoring trips or the use of third-party monitoring.

Any allegations of criminal behavior should be reported to relevant authorities, whether from private or public security, employees or contractors. It is important that allegations related to security personnel be investigated by a neutral party and that any allegations of retaliation be immediately investigated. Confidentiality of complainants must be protected.

If significant changes are needed to prevent recurrence of a verified violation of the Code of Conduct, Bank staff should discuss with the Borrower whether an update is needed to the ESCP, SMP or other relevant documents to include changes or additional corrective actions. Agreed actions should be included in monitoring and supervision, and a summary included in communications with stakeholders, where appropriate.

Gender considerations

If gender-based violence or sexual exploitation and abuse issues arise or are alleged during project implementation or supervision, Bank Management must be alerted immediately. Bank staff are advised to consult the Bank's Good Practice Note on Recommendations for Addressing Gender-based Violence in Investment Project Financing involving Large Scale Civil Works, and to discuss the issue with specialized social development staff. Grievances that deal with gender-related allegations must be handled very carefully, with respect for the confidentiality of the complainants, survivors and their families.

Annex 1: Resources

UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials:
www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

UN Code of Conduct for Law Enforcement Officials:
www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx

Voluntary Principles (VPs) on Security and Human Rights: http://www.voluntaryprinciples.org/what-are-the-voluntary-principles/

ANSI's Management System for Quality of Private Security Company Operations:
http://www.acq.osd.mil/log/ps/.psc.html/7_Management_System_for_Quality.pdf

Armed Conflict Location & Event Data Project (ACLED, which has a useful risk dashboard tool:
https://www.acleddata.com/

International Finance Corporation (IFC) Handbook on the Use of Security Forces: Assessing and Managing Risks and Impacts, 2017 (available in English, French, Spanish)
https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces

International Association of Oil and Gas Producer's Report on Firearms and the Use of Force:
http://www.ogp.org.uk/pubs/320.pdf

MIGA's Implementation Toolkit for Major Project Sites:
https://www.miga.org/documents/vpshr_toolkit_v3.pdf

Voluntary Principles Implementation Guidance Tool: http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf (English);
http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/IGT-SPANISH1.pdf (Spanish)

ICRC and DCAF's Security and Human Rights Toolkit:
http://www.securityhumanrightshub.org/content/toolkit

University of Denver's Private Security Monitor: http://psm.du.edu/

USAID OFDA safety and security update: https://reliefweb.int/sites/reliefweb.int/files/resources/USAID-OFDA%20Safety%20and%20Security%20Sector%20Update%20-%20FY%202017.pdf

Voluntary Principles on Security and Human Rights: http://www.voluntaryprinciples.org/resources/
US State Department: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html

WORLD BANK RESOURCES

World Bank Corporate Security Department
http://workgroup.worldbank.org/org/units/GSD/GSDCS/Pages/Travel-Security.aspx

World Bank Corporate Security Courses
http://workgroup.worldbank.org/org/units/GSD/GSDCS/Pages/Course-Offerings.aspx

Annex 2: Security Management Plans

There are many types of Security Management Plans, from a very general level to very detailed, depending on the needs identified in the SRA. Most SMPs will have the following sections, which will be reviewed at least annually and after any incident, and updated as needed, throughout the project's life.

A. OBJECTIVES AND APPROACH

1. Objectives of an SMP.
2. Security policy description, including priorities, roles and responsibilities. If applicable, describe the relationship between, and relative responsibilities of, project security and other third-party contractors and affiliated contractors, such as the Engineering, Procurement, and Construction contractors.
3. Summary of security approach that can be shared with local stakeholders, including link to the Stakeholder Engagement Plan (SEP) and project grievance mechanism.

B. STANDARDS and GOOD INTERNATIONAL PRACTICE

Refer to standards, requirements and good international practice reflected in the plan. Include national laws, applicable international laws, World Bank Environmental and Social Standards, and other relevant international good practice (see Annex 1).

C. OVERVIEW OF SECURITY SITUATION

1. Project Setting: Relevant demographic information, such as population age, unemployment, poverty, and inequality; crime levels and type; endemic political, social, or labor unrest; terrorism or insurgency; and general attitude toward the project and associated issues.
2. Security Risks: This section should be based on the project SRA and should discuss:
   a. Internal Risks (e.g., illegal, unethical, or inappropriate behavior of project personnel or those directly affiliated with it, such as employee theft, workplace violence, and labor unrest, potentially with associated sabotage).
   b. External Risks, such as those caused by the actions of people outside the project who seek to take advantage of opportunities presented by the development and operation of the project, such as common criminal activity; disruption of the project for economic, political, or social objectives; and other deliberate actions that have a negative impact on the effective, efficient, and safe operation of the project. In extreme cases, these could include terrorism, armed insurgency, coups, or war.

   The SMP should note that a security response or presence of security forces might result in additional risks to communities or individuals.
3. Security Arrangements: Describe who provides basic project-site protection, such as the project private security force (in-house or contracted) and/or arrangements made with public security. Outline agreed Code of Conduct.

D. PHYSICAL SECURITY

Provide an overall description of the project security approach and systems. Ideally this section includes a description of security barriers, such as fences, gates, locks, guard posts, surveillance/electronic security systems used, and a description of the overall security management system.

E. SECURITY OPERATING PROCEDURES

Provide a brief description of key security operating procedures. Key procedures should include a brief description of the following:

- Boundary Security—how security will maintain control of the project's perimeter and channel people to access-control points.
- Access-Point Operations—the types of checks and screening for both people and vehicles at gates or other access points. Include entry and exit searches and purpose, and who is subject to them.
- Incident Response—how security will respond to an incident and who is responsible for responding. Responses should be based on proper and proportional use of force. Describe the role of public security, including when they are called and by whom, for example, regarding criminal activity.
- Security Patrols—what patrols check and how often.
- Travel Security—(if applicable) any special procedure for off-site travel security.
- Materials Storage and Control—(if applicable) any controls over the transport, inventory, and maintenance of storage areas for raw materials, equipment, etc. Note that these are stored in accordance with appropriate national laws and regulations and relevant good international industry practice, including the World Bank Group Environmental, Health and Safety Guidelines.
- Information and Communication—procedures for categorizing, handling, and controlling sensitive information.
- Firearms Security—project policy regarding firearms on-site, as well as the responsibilities and procedures for issuing and storing any security firearms, ammunition, and non-lethal weapons. This should include: location for storage; how weapons are properly secured during storage; records for issuance; who they may be issued to; safeguarding while in possession of the personnel; and audits.
- Special Situations – There may be instances where large-scale events (e.g., criminal activity, demonstrations, civil disorder) require interventions by public security which is not specifically associated with the project. When planning for such events or emergencies, there should be clarity on how project security (private or public) passes control over to formal public security (for example, police, military, emergency responders).

F. SECURITY SUPERVISION AND CONTROL

1. Management Structure and Responsibility, including overall lines of control, accountability, and supervision for the security effort. Define who supervises daily performance of the security force

and who has authority. Describe who has overall responsibility for security information sharing and communication.

2. Responsibility for Conducting Security Risk Assessments: Discuss the responsibilities for conducting risk assessments, who participates in them (e.g., senior management, community relations team, key stakeholders from communities, etc.), and what the assessments cover.
3. Cross-Functional Coordination: Describe interdepartmental coordination, community relations, human resources, and government relations are important partners in project security. Outline any planning/coordination activities between security and other departments, which may range from participation in security risk assessments to weekly meetings.

G. PRIVATE SECURITY MANAGEMENT

Private security's role is to provide preventive and defensive services, protecting workers, facilities, equipment, and operations wherever they are located. Private security personnel have no law-enforcement authority and will not encroach on the duties, responsibilities, and prerogatives reserved for public security forces.

1. Provision and Composition of the Private Security Personnel: Describe whether security personnel are direct employees or from a third-party security provider.
2. Contract Provisions: Include any provisions (e.g., for uniforms and equipment).
3. Active Oversight of Contractor Performance: To ensure proper performance, the project will undertake audits, assist with training, inquire into any credible allegations of abuse or wrongdoing, and monitor site performance on an ongoing basis.
4. Security Personnel Background Screening: The project will perform and/or require its security provider to perform valid background checks on potential security personnel to screen for any allegations of past abuses, inappropriate use of force, or other criminal activity and wrongdoing. No individual for whom there is credible negative information from these checks will serve on the project. These checks will be documented and maintained in individual personnel records, which are subject to review by the project and during project supervision.
5. Security Personnel Equipment: Describe equipment to be provided to personnel, including radios, nonlethal weapons, and any firearms and ammunition. Security personnel should only be armed if it is justified by the SRA is the only viable and effective mitigation measure for a clear threat.
6. Use of Force by Security Personnel: The use of force by private security is only sanctioned when it is clearly for preventive and defensive purposes and in proportion to the nature and extent of the threat. When it is necessary to arm security personnel, the project will ensure that those who are armed exhibit high levels of technical and professional proficiency and clearly understand the rules for the use of force. This means being properly trained on using force effectively, proportionality, and consistent with good international practice, applicable laws and the ESSs.
7. Security Personnel Training:
   - Outline the training responsibilities of either the security provider or the contractor, as applicable. The project will review any third-party security provider's training program and,

where necessary, augment the training through the use of qualified third parties or direct instruction.

- The project will ensure that security personnel receive procedural or knowledge training in: basic guarding skills, guard-post orders and procedures, proper conduct and ethics/human rights, rules of engagement, rules for the use of force, adequate weapons training (as applicable), health, safety, and environment mandatory training, and training on the SEP and relevant public and worker grievance mechanisms.
- Outline how training completion records will be kept. Training will be open to inspection/audit.

H. PUBLIC SECURITY

1. Document Public Security Personnel Role: Summarize the memorandum of understanding or other agreement with public security, including commitment to the project's Code of Conduct and outlining disciplinary action process.

   If public security personnel are assigned to the project to provide some aspects of security, then this section should describe provision of any equipment or other support, the role of the public security force, joint contingency planning, and coordination mechanisms.
2. Provision and Composition of the Security Personnel: Clarify the reporting structure of the security detail and management contact points.
3. Summarize the MoU or agreement for services and request a high-level contact point for security.
4. Monitor security performance on an ongoing basis.
5. Security Personnel Background Screening: The project will agree with public security how individuals assigned to the project will be properly vetted, including how any allegations of past abuses, inappropriate use of force, or other criminal activity and wrongdoing will be taken into account prior to allowing an individual to be assigned to the project.

1. Security Personnel Equipment: Describe equipment to be provided to guards, including vehicles, radios, nonlethal weapons, and any firearms and ammunition.
2. Security Use of Force: Agree with public security providers on the project's principles regarding use of force, to be sanctioned only when it is clearly for preventive and defensive purposes in proportion to the nature and extent of the threat. The MoU or other legal agreement should state that those who are armed must exhibit high levels of technical and professional proficiency and clearly understand the rules for the proportional use of force.
3. Security Personnel Training: Provide opportunities for training or observing project training regarding the project Code of Conduct, health and safety requirements that relate to the project, and the public and worker grievance mechanisms. Outline how training completion records will be kept.
4. Allegations of Misconduct: Agree on how investigations into any credible allegations of abuse or wrongdoing will be undertaken and how discipline for violations of the project Code of Conduct or other project requirements by security personnel will be handled.

Annex 3: Planning and implementing site visits to monitor security risks and arrangements

A. PLANNING THE SITE VISIT

In conflict areas, mission planning starts with the security clearance:[3]

- Ensure advance coordination with the World Bank Corporate Security Office: includes security briefings and resources;
- Particularly in fragile/conflict settings, the Country Management Unit/Country Office Security Specialist should be included as a project team member. The Security Specialist is probably the most skilled on security concerns in the Country Management Unit;
- UN security clearance, as necessary (in the site to be visited)**;**
- Seek the timely approval of the Country Director in principle for the visit. If the response is positive, security and logistical arrangements can be finalized.

Schedule meetings with key personnel: As part of scheduling meetings and the required Security Briefings, ensure that relevant site management personnel are included to be able to provide and discuss security-related information, including:

- General Manager, Project/Site Manager/Director (who has overall responsibility for project risks);
- Security/ Asset Protection Manager (or person responsible for security);
- Community Relations Manager;
- Human Resources Manager, Environmental Health and Safety Manager.

Request assistance in arranging meetings with external stakeholders, including, as appropriate:

- Public Security representatives, where possible and appropriate (e.g., local senior police officer, regional military commander, etc.);
- Local public authorities (divisional officers, sub-divisional officers; etc.);
- Municipal authorities;
- Development partners such as UN agencies;
- Community members:
    - Seek information on community members' concerns, where possible;
    - If the topic of security personnel may be raised, it is good practice to **not** have security personnel present during meetings with community members or civil society, even if this means that a meeting location needs to be switched to a more neutral location. Community members may be reluctant to be forthcoming with information or complaints if the security personnel they are concerned about are present in the meeting or if word reaches them on who has complained. Safety for complainants is critical and they should not be made to feel more vulnerable because they have used a grievance mechanism or raised a concern;
    - Reiterate the commitment to the Code of Conduct and grievance mechanisms that apply to the project;

[3] The purpose of the GPN is not to address issues of security related to Bank staff and missions. For further information, contact the World Bank Corporate Security Office (http://security/).

- Civil society (national and international NGOs).

B. CONDUCTING A SITE VISIT – OBSERVATIONS

Observations on site: Site visits provide the opportunity for many useful observations about security while arriving at and moving around the site. There should be an advance briefing about the project activities, sites, and security issues that may help focus questions and observations. It is important to look for:

- Security provisions on site, such as:
    - Visible private security presence in and around the site;
    - Visible public security presence in and around the site;
    - Are there any women security personnel? (This can be particularly relevant and helpful if there are expected interactions between project workers and the local community, or between female workers or visitors and security staff, such as inspections);
    - In case of the use of armed security, is their uniform different from other uniformed project personnel?
- Professionalism of security guards, for example:
    - Proper uniforms, clean cut;
    - ID with prominent photo and name;
    - Basic stance, posture, demeanor.
- Weapons and serviceable equipment:
    - Are (private or public) security personnel carrying weapons?
    - If they have firearms, are pistols properly holstered and long weapons properly controlled?
    - Are there guard dogs? Are they well-controlled/restrained? Do they appear to be well-trained?
    - Are private security personnel using properly identifiable company vehicles or equipment? Are public security personnel using properly identifiable company vehicles or equipment? Do they have identifying badges that show they are linked to the project?
- What communications equipment are on their person and otherwise available?
- Medical Evacuation (MEDEVAC): Is there an established medical evacuation procedure?
- Facilities:
    - Are there any facilities provided to security personnel (including any welfare and accommodation facilities)?
    - Are there secured storage areas/facilities for weapons not in use?
- Access points and signage:
    - Are there clear signs about protocols (including safety messages)?
    - Is the name of the project and contact information prominent at access points?

  - Is there emergency contact information listed if someone needs to report an incident or emergency?
  - Are there procedures in place to ensure people are not bringing weapons or other prohibited materials (e.g., alcohol, drugs) or unauthorized persons on site?
  - Are there procedures in place to ensure project property or vehicles are not improperly removed from site?
  - What types of barriers (for example, fences) are being used, if any?

Observations off site: Observations outside the site, for example travelling from the airport or capital city to the site, or within the local community, can help form an important picture of the security landscape. The following should be discussed with the Borrower:

- Public security: quality and presence in the capital city vs. local/remote areas;
- Local community activities:
  - Behavior of and towards women and children;
  - Local commerce (e.g., market activity);
  - Public routines and curfews;
  - Local daily life vs. current reality (i.e., find out what is usual, and assess whether what is observed conforms to that description).

C. SITE VISIT – QUESTIONS

Additional information should be derived from asking questions of many different stakeholders. This can help gain new information as well as confirm previously collected information or insights. This section offers a wide range of potential questions: select/modify what may be relevant to the project and context. Questions during project implementation should aim to assess understanding of the essential elements of the security arrangement prepared for a specific Bank project (e.g., any codes of conduct, training content, protocol of security responses, reporting procedure), what the security response has been to past incidents, and issues in implementing the security arrangement/security management plan.

If there is an anticipated transition at the project, such as from construction to operations, questions (to many of the individuals listed below) should be asked about the change in security risks and security management that will accompany this transition.

Questions for Security Personnel: Security incidents can occur when the security personnel themselves do not feel secure. It can be helpful to establish how the site security guards perceive their job, the community and their employer, as well as how they conduct their duties. These answers can be compared to the security procedures provided by the Borrower. If opportunity permits, talk to individual security personnel about the following:

- Employment context: duties, wages, length of shift, food rations, duration of employment, training;
- Supervision and reporting: who their manager is, where they would report/escalate incidents;
- Basic scenario-based questions:
  - What would they do first if someone forced their way onto the property?
  - What would they do if someone stole something and was running away?

  - What type of interaction(s) do they typically have with community members, if any?
  - What is a typical day on the job like?
  - What is a typical work schedule? (e.g., how many shifts per day/week?
  - What is the duration of day and night shifts?

- Be aware that if the project provides an interpreter or translator, the responses to questions may be communicated back to the project team or security management. In a high-risk area, or where security concerns have been identified, it may be useful to have a neutral translator instead of one supplied by the project.
- Try to clarify if the security personnel are affiliated with a particular community or group, and whether it is the same as that of people in the project area or different, and if this has raised any tensions.

Questions for Community Members: Women with children can often provide a good indication of how community members, especially those more vulnerable, feel about security in their communities and how the community perceives security personnel. Every meeting context is different, so not everyone will feel comfortable engaging. Potential questions include:

- To whom would you report a problem or an incident or crime? [Often, not everyone will have heard of the grievance mechanism, but they should know someone in authority who would be aware of it.]
- If your child was injured or hurt - would you tell them to approach the police, or to avoid them?
- Have you heard or experienced any problems or incidents associated with the project? (Keep open-ended and note if any issues regarding security are raised. Do not specifically focus on security if not raised, and include in more general discussion on grievance management.)

Discussion with the General Manager or Project/Site Manager: Understanding how the General Manager or Project/Site Manager views the community and security risks will be crucial to the success of identifying and managing security issues on site. This person(s) is unlikely to know all the details about security management, but both the content and delivery of responses to questions can provide a perspective on the relevance, attention and support that security is given at the higher level. Topics for discussion may include:

- Site security risks;
- How the site is protected;
- Security of the local community;
- Relationship with local community and any initiatives;
- Potential use of national security forces, and if not proposed, clarification on the point at which escalation in security risks may require outside assistance, what discussions have been held to identify thresholds for additional support and if there are agreed transition procedures in such an event;
- Existence of an early warning system.

Questions for the Security Manager: Not every site will have a dedicated Security Manager, but someone will be responsible for security. This person should be able to confidently answer questions such as:

- How is the SMP implemented?

- Has the SMP been reviewed recently? Are there any changes needed?
- Has the SRA been updated with any new issues? What are they and how are they being handled?
- How are personnel trained on the Code of Conduct? How often?
- What issues have been raised in grievances from workers or the public with regard to security personnel? What happened in these cases?
- Have any high-risk or red-flag zones on security been identified?
- Have there been any recent security alerts, advisories or restriction of movements?
- What is the relationship/interaction with public security? When would it become involved?
- Are there any concerns about public security personnel in general? Any concerns about public security personnel's ability to act in a manner that is consistent with international good practices, applicable laws and the ESSs?
- What is the frequency of consultation with community relations/human resources/environment team on security-related matters?
- What are the security interactions with the local community? Have there been any incidents? What are the reporting and investigation procedures for incidents?
- What is the background and employment process for private security guards (including private contractors)?
    - Training schedule and program for guards (and public security, if applicable)?
    - Relationship between the SMP and the ESMS, ESMP, SEP, etc.?

Questions for the Community Relations Manager: A good working relationship between the community relations and security teams can significantly improve mitigation of possible security risks both from and to the community. This discussion is likely to provide useful information about security, as well as many other issues relevant to the community. Questions for the person responsible for community relations may include:

- What is the relationship with the Security Manager/security team?
- What is the relationship between the SMP and the ESMS, ESMP, SEP, etc.?
- What has been the nature of interactions between community and security?
- What is the community perception of public security in the area?
- What have been the community complaints or incidents related to security?
- Are grievance mechanisms available to the community if a security incident occurs?
- If so, how are grievances reported (e.g., is it an accessible process) and how are they investigated and followed up on?
- Does the grievance mechanism allow a woman complainant to speak to a woman in the project team?

Questions for EHS Manager/Supervising Engineer:

- What do you understand your role to be in relation to security contracts and arrangements?

- What are the typical interactions of Engineering, Procurement, and Construction contractor/sub-contractors/service providers with security personnel (e.g., access point, gate control, etc.)?
- What are the key security risks (at the project site, at any other remote construction site or camp, in transit)? Do you have any concerns about the ability of security personnel to respond appropriately to such risks?
- Are you aware of a security management plan? Does it include workers/ contractors? Who manages it? How often is it reviewed and updated (e.g., routinely and after any incident)?

Questions for Public Security: Public security may include the head of the local police, military, or gendarmerie supervisor. Questions for/about public security include:

- Has the project increased your workload in the area?
- Do you have a relationship with the project team that enables you to promptly and clearly share concerns?
- Do you feel the project team recognizes your concerns?
- What kind of incidents have occurred —can you give some examples?
- Are the security personnel on rotation? For how long are they assigned to the project security? When new personnel are rotated in, what kind of training is provided?
- How do the security forces interact with the local community?