Annex 21 - Assessing and Managing 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.*   1. *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.* 2. *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.* 3. *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.”* |

***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, socioeconomic 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 deescalate, 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.

**USE OF MILITARY FORCES TO ASSIST IN COVID-19 OPERATIONS**

**SUGGESTIONS ON HOW TO MITIGATE RISKS**

1. **WHAT ARE THE THINGS TO WATCH FOR?**

* 1. ***Diversion of materials, aid and assistance*:** Diversion can take the form of confiscations and reuse, misappropriation and theft. While a certain level of diversion may be inevitable in certain circumstances, this issue is likely to present reputational issues (especially when the crisis dissipates).

* 1. ***Allegations of human rights violations:*** This will be a risk, including as it relates to Sexual Exploitation and Abuse and Sexual Harassment (SEA/SH), and the Bank needs to be clear and transparent about what measures are being adopted to minimize these risks. Tools that should be considered include the ESF Good Practice Note (GPN) on [Use of Security Forces,](http://documents.worldbank.org/curated/en/692931540325377520/Environment-and-Social-Framework-ESF-Good-Practice-Note-on-Security-Personnel-English.pdf) on [SEA/SH,](http://pubdocs.worldbank.org/en/632511583165318586/ESF-GPN-SEASH-in-major-civil-works.pdf) and the IFC Good Practice Handbook on the [Use of Security Forces: Assessing and Managing Risks and Impacts.](https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces)

* 1. ***Putting World Bank staff at risk*:** This is particularly a concern where military/security forces are likely to be undisciplined. The risk may be heightened when Bank staff are trying to address the risk of diversion referred to above. While staff may try to address this risk by avoiding direct interaction with the military, this is not likely to be feasible in a project setting.

* 1. ***International media comment and reaction***: This will be a challenge, and it may not be possible to avoid negative comment entirely. It is important to be transparent about the activities the World Bank is supporting and the mitigation measures that are being implemented to address risks.

1. **WHAT ARE THE WAYS TO ADDRESS THE RISKS?**

* 1. ***Get a view of the reputation and capability of the military*:** Talk to those who might have up to date and accurate information:e.g. the Defense Attaché at the relevant Embassy; the US or UK Government; refer to Jane’s Defence Weekly.

* 1. ***Identify the structure under which the military will be******operating***: While they will continue to abide by their own rules and procedures, it is likely that the military will also be subject to relevant national requirements relating to the public health emergency and the specific activities that they are required to carry out e.g. instructions issued by public health officials. In the context of a Banksupported operation, it is good practice to document (as far as possible) the structure under which the military are operating, including the chain of command, with specific reference to the activities they will or are likely to carry out (see paragraph (i) below).

* 1. ***Clarify who is responsible for human rights issues nationally*:** Many countries have a Human Rights Commission. If such commissions do not exist, there is usually an Ombudsman, Human Rights office or inspector general at the national level with jurisdiction to deal with such issues. Identify the relevant parties and consider whether it would be appropriate to consult them for advice.

* 1. ***Identify other specialized parties and ask for advice***: There are both national and international NGOs which follow and support these issues (e.g. Human Rights Watch (HRW), Amnesty). There is also the International Committee of the Red Cross (ICRC) and the International Crisis Group. Identify relevant parties, with reference to the context and nature of the operations, who may be in a position to provide valuable advice.

* 1. ***As required under the ESF, cooperate with relevant stakeholders on a risk assessment*:** Carry out a risk assessment to identify the specific risks associated with the proposed use of military. This assessment needs to be conducted with those that are involved in the operation, including Government counterparts, to ensure that an accurate picture of the risks emerge, that appropriate mitigation measures are identified and that both the risk assessment and the mitigation measures are owned by the project and the Government.

* 1. ***Be transparent about what the World Bank is requiring to mitigate the risks***: Document this, setting out key aspects in the ESRS and other project documentation. Consider the following:
  + procedures relating to: e.g. risk assessment; how allegations of HR/SEA/SH violations will be dealt with, including through the project Grievance Mechanism (GM); preventing diversion of materials, aid and assistance (build on existing requirements)
  + presence of World Bank representatives/third party monitors on the ground
  + cooperation with specialist institutions/NGOs/Government agencies
  + specific obligations set out in the legal agreement and (if possible and appropriate) a Memorandum of Understanding (see paragraph (k) below)
  + monitoring and reporting

1. ***Consider asking a credible party to act as an observer/third party monitor***: This can be considered under the ESF provisions for third party monitoring as noted in ESS1 and ESS10, as well as the ESF Good Practice Note on Third Party Monitoring. Relevant groups with experience in this field will depend on the context, and may include the parties referred to in paragraph (d) above.

1. ***Establish a procedure to be followed in cases of allegations of HR/SEA/SH violations or misbehavior***: This should reflect the ESF Good Practice Note on SEA/SH and may include reference to the institutions referred to in paragraph (c) above. Include a specific HR and SEA/SH procedure in the project GM to address these allegations and identify specific individuals who have the expertise to address such allegations credibly. Understanding relevant Code of Conduct (CoC) requirements pertaining to such behavior is important, and, where necessary, improving the form and substance of such CoC.

1. ***Be clear on what the military will do***: Identify the activities and set them out clearly in the legal agreement: e.g. construction, enforcing quarantine restrictions, distribution of medical supplies or vaccines, distribution of other supplies. This will support a more accurate risk assessment. Note that in some circumstances, what could otherwise be viewed as inappropriate behavior by the military (or at an extreme, a possible abuse of rights) may be authorized and necessary in situations of a public health emergency. This will depend on the activities that the military is required to carry out and will be particularly relevant where they are required to enforce public order or quarantine restrictions.

1. ***Set out specific requirements as covenants in the legal agreement and in the Environmental and Social Commitment Plan (ESCP) as appropriate:*** The provisions should set out the ‘ground rules’ for military engagement, including: (i) requirements to comply with ESS4 (see Annex attached); (ii) reporting obligations (specify on what, how often, to whom); (iii) specific prohibitions e.g. no child labor, no forced labor, restrictions on what military personnel under the age of 18 can do (if anything); (iv) health and safety requirements; (v) Code of Conduct (CoC) type obligations; (vi) requirements for the GM; (vii) training required and how often (specify on what – e.g. Voluntary Principles on Security and Human Rights, interactions with the community, operation of the GM, use of personal protective equipment (PPE), CoC).

1. ***Where possible, and if not already covered by applicable law/regulation, the Government should consider executing a Memorandum of Understanding (MoU) with the military:*** This should reflect the ‘ground rules’ set out in the legal agreement (see paragraph (j) above). An example of a MoU is available in the IFC Good Practice Handbook on the [Use of Security Forces: Assessing and Managing Risks and Impacts.](https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces) Even where it is not possible for individual military personnel to sign a CoC, the requirements should be set out in the MoU, and training should cover these obligations (amongst others).

**Set out below is suggested wording on HR/SEA/SH:**

1. Prior to deploying military or security personnel, the [Borrower/Recipient] shall take measures to ensure that such personnel are:
   * 1. screened to confirm that they have not engaged in past unlawful or abusive behavior, including sexual exploitation and abuse (SEA), sexual harassment (SH) or excessive use of force;
     2. adequately instructed and trained, on a regular basis, on the use of force and appropriate behavior and conduct (including in relation to SEA and SH), as set out in the [*Training Procedure*, *Project Operational Manual, ESMF, Security Management Plan, MoU* ]; and
     3. deployed in a manner consistent with applicable national law.
2. The [Borrower/Recipient] shall promptly review all allegations of unlawful or abusive acts of any military/security personnel, take action (or request appropriate parties to take action) to prevent recurrence and, where necessary, report unlawful and abusive acts to the relevant authorities.

**Set out below is suggested wording on reporting:** Frequency of reporting will depend on the context and the risks associated with the activities the military is carrying out, and may be required monthly, weekly or even daily. Requirements should include:

* + Immediate reporting (within 24 hours) of any serious incident
  + A written weekly or monthly report (depending on the risk) covering:
    - * status of activities being conducted by the military o training conducted (specifying subject matter)
      * current status of review of serious incidents (if any) and any relevant reporting o a summary of any minor (but reportable) issues, suspected incidents or potential issues o details of any incidents involving use of force or weapons
      * details of upcoming activities which may pose a risk (e.g. distribution of supplies) and measures being put in place to reduce such risk
      * lessons learnt, to inform conduct of future activities

**Other reference documentation**: [The International Code of Conduct under the Montreux Document.](http://www.icoca.ch/en/the_icoc) While this relates to private security, it contains useful material.