

**Document Name**  
Security Management Plan

**ETHIOPIA-SOMALILAND  
NORTHERN HIGH VOLTAGE  
INTERCONNECTOR:  
ETHIOPIA**

**SECURITY MANAGEMENT  
PLAN FOR 71.3KM JIGJIGA  
TOGO WAJAALE HIGH  
VOLTAGE TRANSMISSION  
LINE.**

## ACRONYMS

ASP	Activity Security Plan
CoC	Code of Conduct
EAPP	Eastern Africa Power Pool
ESF	Environmental and Social Framework
ESHS	Environmental, Social, Health and Safety
ESIA	Environmental and Social Impact Assessment
ESMF	Environmental and Social Management Framework
GBV	Gender Based Violence
GIIP	Good International Industrial Practices
GRMs	Grievance Redress Mechanism
IED	Improvised Explosive Devices
IGMOU	Inter-Governmental Memorandum of Understanding
OHS	Occupational, Health and Safety
PBIED	Person Born Improvised Explosive Devices
PIU	Project Implementation Units
RoW	Right of Way
RPG	Rocket-Propelled Grenade
SEA	Sexual Exploitation and Abuse
SMP	Security Management Plan
SRM	Security Risk Model
UNSMS	UN Security Management System
VBIED	Vehicle Born Improvised Explosive Devices
WB	World Bank

# TABLE OF CONTENTS

ACRONYMS .....	2
TABLE OF CONTENTS .....	3
LIST OF TABLES .....	4
LIST OF FIGURES .....	4
EXECUTIVE SUMMARY .....	5
<b>1 INTRODUCTION.....</b>	<b>7</b>
<b>1.1 PROJECT DEVELOPMENT OBJECTIVES.....</b>	<b>7</b>
<b>1.2 PROJECT COMPONENTS .....</b>	<b>7</b>
1.2.1 Component 1-Physical Interconnection Infrastructure .....	7
1.2.2 Component 2-Energy Access Interventions in Borderland Areas .....	7
1.2.3 Component 3-Technical Assistance and Capacity Building for Regional Power Integration.....	7
<b>1.3 PROJECT OVERVIEW .....</b>	<b>8</b>
<b>1.4 RATIONAL FOR SECURITY MANAGEMENT PLAN .....</b>	<b>8</b>
<b>1.5 PURPOSE OF SECURITY MANAGEMENT PLAN.....</b>	<b>9</b>
<b>1.6 SECURITY RISK ASSESSMENTS AND MANAGEMENT PLAN OBJECTIVES.....</b>	<b>9</b>
1.6.1 Specific Objectives .....	9
1.6.2 Security Risk Assessment Methodology and Scope .....	10
<b>1.7 PROJECT PROPONENTS AND IMPLEMENTATION ARRANGEMENTS.....</b>	<b>10</b>
1.7.1 Ethiopian Electric Power .....	10
1.7.2 Eastern Africa Power Pool.....	10
<b>2 LEGAL FRAMEWORK.....</b>	<b>12</b>
<b>2.1 NATIONAL POLICES AND LEGAL FRAMEWORKS.....</b>	<b>12</b>
2.1.1 Provisions of the Constitution of Ethiopia.....	12
2.1.2 Ethiopia’s Labour Proclamation No. 1156/2019 .....	15
2.1.3 Proclamation on Gender Based Violence and the Ethiopian National Policy on Women.....	16
<b>2.2 WORLD BANK ENVIRONMENTAL AND SOCIAL FRAMEWORK REQUIREMENT</b>	<b>17</b>
2.2.1 ESS1: Assessment and Management of Environmental and Social Risks and Impacts .....	17
2.2.2 ESS2: Labor and Working Conditions.....	18
2.2.3 ESS4: Community Health and Safety .....	18
2.2.4 World Bank’s Good Practice Note on Assessing and Managing Risks of the use of Security Personnel .....	19
2.2.5 World Bank Group (WBG) Environment, Health and Safety (EHS) Guidelines .....	20
<b>2.3 INTERNATIONAL STANDARDS AND GOOD PRACTICE.....</b>	<b>20</b>
<b>3 SECURITY CONTEXT AND THREAT ASSESSMENT .....</b>	<b>22</b>
<b>3.1 NATIONAL SECURITY CONTEXT .....</b>	<b>22</b>
<b>3.2 SECURITY CONTEXT IN TRANSMISSION LINE PROJECT ROUTE.....</b>	<b>23</b>
3.2.1 Nature of Risks/Conflicts .....	23
<b>4 SECURITY RISK ASSESSMENT.....</b>	<b>24</b>
<b>4.1 METHODOLOGY OF THE SECURITY RISK ASSESSMENT.....</b>	<b>24</b>
<b>4.2 OBJECTIVES OF ASSESSING SECURITY RISKS .....</b>	<b>25</b>
<b>4.3 RISK ASSESSMENT APPROACHES.....</b>	<b>25</b>

4.3.1	Security Risk Trend Assessment .....	25
4.3.2	Current Security Condition Assessment.....	26
4.4	SECURITY RISK IDENTIFICATION .....	26
4.4.1	Internal Security Risks .....	26
4.4.2	External Security Risks .....	27
4.5	DATA COLLECTION MAIN FINDINGS .....	27
4.6	MAIN SECURITY THREATS.....	28
4.7	SECURITY RISK ANALYSIS AND EVALUATION.....	31
5	SECURITY RISK PREVENTION AND MITIGATION .....	34
5.1	APPROACH TO MANAGING SECURITY RISK .....	34
5.1.1	Development of the Approach .....	34
5.1.2	Phased Approach .....	34
5.1.3	Additional Measures.....	34
5.1.4	Adaptation and Monitoring .....	34
5.1.5	Security Risks Mitigation Measures.....	35
6	SECURITY APPROACH .....	40
7	SECURITY MANAGEMENT ARRANGEMENTS .....	42
7.1	OVERSIGHT AND CONTROL OF SECURITY OPERATIONS .....	42
7.2	COMMUNITY ENGAGEMENT .....	43
7.3	SECURITY MANAGEMENT AND MONITORING PLAN.....	43
8	ANNEX .....	52
8.1	SECURITY OPERATING PROCEDURES.....	52
8.2	ESCALATION MATRIX .....	56

## LIST OF TABLES

Table 2—1.	Relevant Constitutional Provisions-Ethiopia.....	13
Table 4—1.	Category of Workers.....	30
Table 4—2.	Threat Scenarios.....	30
Table 4—3.	Likelihood of Risk Occurrence.....	31
Table 4—4.	Risk Severity descriptions and rating .....	31
Table 4—5.	Risk Matrix and Score Range .....	32
Table 4—6.	Security Risk Identified .....	32
Table 5—1.	Operational Health and Safety Risks and Mitigation Measures .....	36
Table 7—1.	Security Management Plan .....	44

## LIST OF FIGURES

Figure 1-1:	Transmission Line Route Jigjiga-Togo Wajaale.....	8
Figure 3-1.	Security Hotspots in Ethiopia.....	22

## EXECUTIVE SUMMARY

The proposed construction of the 73.1km High Voltage (HV) Jigjiga-Tog Wajaale 400kV double circuit transmission line ('the Project') starting from Jigjiga substation (250877.74 m E; 1039897.48 m N) and terminating at Tog-Wajaale in the Somali region (312271.34M e E1067373.63 m N) at the border between Ethiopia and Somaliland. The transmission line crosses one Zone (Fafan), 4 Woredas and 14 Kebeles found in the Somali Regional State. The proposed Right of Way (RoW) for the transmission line will be approximately 40 metres wide.

The security risk assessment and management plan is prepared with objective of to assess and identify the potential security risks that could potentially threaten the safety and security of the program workers and the beneficiary community in the program intervention areas. The specific objectives are highlighted in the next sub section. Both primary and secondary data were used for the preparation of the document.

In the project transmission line route, there are security risks that emanate contextual circumstances for instance government attempt to enforce laws in the Northern part of the country; relation with local community which could be manifested by relationship between the contractors and community, the contractor and workers, the Eastern Africa Power Pool (EAPP) Project Implementation Unit (PIU) and Ethiopian Electric Power (EEP-PIU) and community; and impacts of incidents and response to incidents and other. Security threats/risk can either be external or internal.

Based on the finding from the security risk assessment the potential external security risks include the following:

- Theft of equipment and material: employee or visitor/guest stealing equipment or material from project site or individual house.
- Burglary: Illegal entry of a building with intent to commit a crime, especially theft. It involves breaking and entering the premises. This can be done by staff or outsiders.
- Banditry/Roadside attacks on workers during transit: The project can be susceptible to attacks while transporting equipment and materials to the targeted regions or to project workers when travelling for field activities.
- Community unrest: Due to influx of labor, improper behavior towards the community, land and water use conflict, improper site selection and locating project infrastructures and associated facilities, resource abuse by the contractors, improper waste disposal, noise and dust pollution, etc.,
- Risks from employee industrial action and disruption of services: Likely cause for labor disputes include demand for limited employment opportunities; labor wages/rates and delays of payment; disagreement over working conditions, raising concerns regarding unsafe or unhealthy work situations, or any grievances raised, and such situations could lead to labor unrest and work stoppage.
- Gender-Based Violence (GBV)/sexual exploitation and abuse (SEA) and gender-based security incidents. This becomes a security issue when GBV/SEA is inflicted by perpetrators to women and girls of the project workers and community in the project areas (Please refer GBV Action Plan).

- Risks emanating from the use of security personnel: Use of security personnel may exacerbate tensions. Security personnel can be private or public. Security personnel can be engaged by the project contractor. Their presence can pose risks to, and have unintended impacts on, both project workers and local communities. Examples include committing a GBV/SEA act by security personnel within conflict affected work environment. It can also occur during community unrest and actions ethnic conflicts within the work environment.
- Risks associated with armed conflict and kidnapping: armed conflict between government and non-government forces and between non-government armed forces. In areas in which armed groups are operating, there are risk of kidnapping.
- Environment and OHS risks: Program activities pose potential Environment and Occupational, Health and Safety (OHS) risks which include exposure to hazardous material, noise and vibration, dust (affecting air quality), wastes, stuck by objects, work in height, fire and risks associated with availability of potable etc.
- Risk of traffic accident: due to erratic driving habits and poorly maintained road infrastructure traffic accidents are potential risks.
- Medical risk: Access to adequate medical and emergency care in rural areas of the country is limited causing medical risks.
- Exposure to natural hazard (flooding): the rainy season in Ethiopia runs from June to September, and during this period flooding is common posing flooding.

# I INTRODUCTION

## I.1 Project Development Objectives

The Horn of Africa Regional Integration for Sustainable Energy Supply (P174175) is a World Bank financed project whose objective is to enhance regional integration of energy supply and to improve energy access in the borderlands in Horn of Africa countries.

## I.2 Project Components

### I.2.1 Component 1-Physical Interconnection Infrastructure

The component will provide support to some or all of the following activities, depending on investment readiness and political buy-in from the client countries: (a) the construction of 400 kV transmission lines between Ethiopia and Somalia (Northern and Southern), (b) the reinforcement of the existing Ethiopia-Sudan 230 kV double circuit transmission line, and (c) the construction of the second Ethiopia-Sudan 500 kV transmission line.

### I.2.2 Component 2-Energy Access Interventions in Borderland Areas

Component 2 targets energy access interventions in borderland areas, mostly agri-pastoralist population in Ethiopia and Somalia. It includes the following activities: (a) electricity access to public institutions (for example, health facilities, schools, veterinary posts, community centers, street lighting, telecom towers), (b) electricity access to households, (c) electricity access for productive uses (for example, water points-which are mostly privately owned-refrigeration and cold chains, agri-processing, and so on), and (d) access to clean cooking for households and social centers in borderland communities of the HoA. Women are expected to benefit disproportionately from the interventions as they have lesser mobility whereas men tend to travel seasonally for livestock trading and are already engaged in cross-border trading activities. This component will also support a benefit-sharing program for the affected communities by Component 1. This component will prioritize the most vulnerable and underserved communities or development nodes<sup>1</sup> where there is lack of energy access, concentrated presence of public institutions and water points along trading routes (places of gathering for surrounding communities, including nomadic population) and markets, and existing cross-border trade.

### I.2.3 Component 3-Technical Assistance and Capacity Building for Regional Power Integration.

Component 3 will provide technical assistance and capacity building to the EAPP, its member countries. This component will be informed by the Regional Power System Master Plan (2014) (RPSMP) of the EAPP<sup>2</sup> and the African Union Program Infrastructure Development for Africa (PIDA) 2020 Priority Action Plan. In addition, proposed activities

---

<sup>1</sup> A development node is defined as a location of strategic importance to maximize the development impact in the area. A development node can be identified by various factors, including, but not limited to, the concentrated presence of services such as water points, education and health facilities; markets (livestock or agricultural markets); communication nodes (telecommunication towers); proximity to trading routes or places of gathering for surrounding communities, nomadic population, and displaced people.

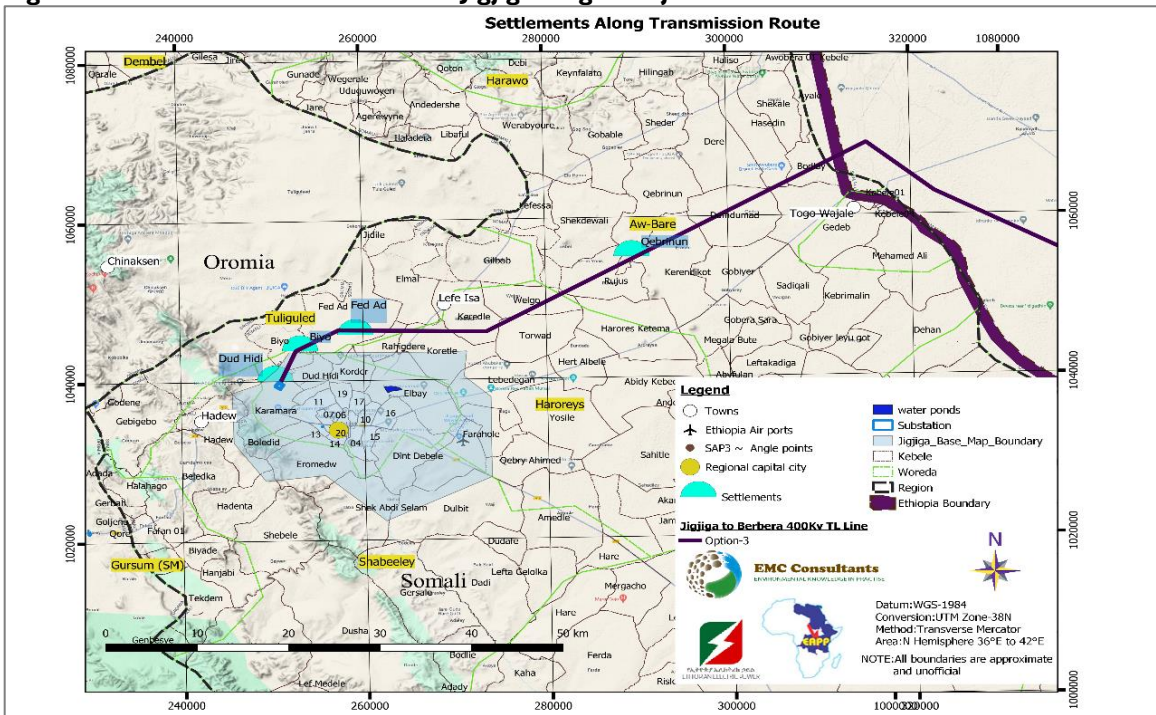
<sup>2</sup> The RPSMP is subject to update, which is expected to start in June 2021.

will be informed by the EAPP 10-year Strategic Plan (2018–2027) and the Short-term Action Plan (2021–2023).

### I.3 Project Overview

The proposed high voltage transmission line traverses Somali Regional State starting at proposed site for construction of Jigjiga substation (250877.74 m E; 1039897.48 m N) and terminating Tog-Wajaale (312271.34m e E1067373.63 m N). The proposed Right of Way (RoW) for the transmission line will be a 40m wide corridor with a total length of 73.1km running suggesting that approximately 292.4ha of land may be acquired and/or expropriated for project purposes.

Figure I-1: Transmission Line Route Jigjiga-Togo Wajaale



Source: EMC Consultants, 2024

Upon completion, the HV 400kV double circuit transmission line will be energized as part of the national grid and will be part of the Ethiopia-Somalia interconnector.

### I.4 Rational for Security Management Plan

The Environmental and Social Framework (ESF) of the World Bank (WB) governs the management of environmental and social (E&S) risks for projects financed by the Bank specifically Environmental and Social Standards (ESSs) 1 and 4 which indicate the need for security protection of the work environment including the requirement to manage risks emanating from engagement of security personnel in the project. ESS 1 of the ESF requires clients to better assess and manage E&S risks and impacts for improvement of financed development outcomes. The WB 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 states that social conflict analysis is an instrument that assesses the degree to which the project may:

- Exacerbate existing tensions and inequality within society
- Have a negative effect on stability and human security.
- Be negatively affected by existing tensions, conflict and instability, particularly in circumstances of war, insurrection and civil unrest.”

ESS4 also addresses the health, safety, and security risks and impacts on project-affected communities and the corresponding responsibility of client to avoid or minimize such risks and impacts, with particular attention to people who, because of their particular circumstances, may be vulnerable. When security personnel are used to provide security to safeguard project’s personnel and property, there is a need to assess risks posed by these security arrangements to those within and outside the project sites. The sanctioning of any use of force by direct or contracted workers in providing security is discouraged except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.

## **1.5 Purpose of Security Management Plan**

This Security management Plan (SMP) has been prepared for the construction of the Ethiopia-Somalia electricity interconnections project. The purpose of the SMP is to provide a blueprint for managing safety and security throughout all phases of the project. It is designed to identify and manage potential security risks for the protection of project employees, visitors, and the project communities. The SMP explains how to respond to potential safety and security incidents like accidents and crimes and also provides a brief description of the roles and responsibilities of staff and workers when incidents occur.

The plan outlines the project’s policies and procedures and identifies general and high security risks with an aim of developing effective responses. The plan proffers mitigating measures based on the specified security levels and the specific activities of the Project. It also outlines how security will be managed, the responsible institutions, and the required resources. Furthermore, it guides the project on how implementation should avoid reinforcing existing conflict stressors but rather leverage opportunities to reinforce resilience to promote peace and stability. In this regard, the primary and secondary data validated some potential security risk factors during project implementation in Somalia.

## **1.6 Security Risk Assessments and Management Plan Objectives**

The overall objective of this security risk assessment and management plan is to assess and identify the potential security risks that could potentially threaten the safety and security of the program workers and the beneficiary community in the program intervention areas.

### **1.6.1 Specific Objectives**

- To identify, evaluate, and prioritize potential security risks and impacts likely to affect the safety and security of persons and operation of the project;
- To understand and respond to community concerns and perceptions

- To determine appropriate security arrangements
- To propose mitigation measures and security management plan for the identified security risks and impacts related to the project.
- To identify potential security risks and impacts to project workers and other stakeholders due to the proposed project interventions, in Somalia
- To define the required resources for the identified actions of the project
- To assess and define the responsible actors, institutions and agencies for the planning and implementation of the SMP

## **1.6.2 Security Risk Assessment Methodology and Scope**

### **1.6.2.1 Scope**

The assessment focusses on the areas that the line crosses i.e. 1 region (Somali)

### **1.6.2.2 Literature Review**

Primary and secondary data were used for the preparation of the document. Secondary data such as review of relevant national legislation and regulations, Good International Industrial Practices (GIIP) for instance ISO 31000 (Risk Management Guidelines) and the WB Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel.

### **1.6.2.3 Primary Data Collection Methods**

The primary data collection methods deployed includes observation in selected villages using interviews, observation and consultations.

## **1.7 Project Proponents and Implementation Arrangements**

### **1.7.1 Ethiopian Electric Power**

The proponent of the proposed High Voltage 400kV transmission line is EEP and was established by the Federal Democratic Republic of Ethiopia (FDRE) Council of Ministers Regulation No. 302/2013 and amended Regulation No. 381/2016.

### **1.7.2 Eastern Africa Power Pool**

The Eastern Africa Power Pool (EAPP) is a regional institution established in 2005 to coordinate cross-border power trade and grid interconnection among nations of the Eastern Africa region. The EAPP currently has thirteen (13) member states that signed the Inter-Governmental Memorandum of Understanding (IGMOU) and fourteen utilities that signed the Inter Utility Memorandum of Understanding (IUMOU). The pool comprises the following countries: Burundi, Djibouti, Democratic Republic of Congo (DRC), Rwanda, Egypt, Ethiopia, Kenya, Sudan, Tanzania, Uganda, and Libya. South Sudan and Somalia joined recently and there's a possibility that Eritrea may join. The EAPP's General Secretariat is based in Addis Ababa, Ethiopia with a mandate to coordinate the development and functioning/operation of the power pool. A Project Implementation Unit (PIU) has been established at the EAPP and will be responsible for the management of the project. The PIU include a Project Coordinator, one FM Specialist, one Procurement Specialist, one Environment Specialists, one Social Specialist and Technical Specialists.



## 2 LEGAL FRAMEWORK

The Security Management Plan is prepared in conformance with both the Constitution of the Federal Democratic Republic of Ethiopia and the 2019 National Labour Proclamation No. 1156 of Ethiopia.

The Security Management Plan is prepared also in conformance with the Environmental and Social Framework (ESF) of the World Bank (WB), which governs the management of environmental and social risks for projects financed by the World Bank. In particular, the Environmental and Social Standards 1 (ESS1) and Social Standard 4 (ESS4) stress the need for security protection of the work environment including the requirement to manage risks emanating from engagement of security personnel in the project.

The World Bank's Environmental and Social Standards 1 (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:

- Exacerbate existing tensions and inequality within society.
- Have a negative effect on stability and human security.
- Be negatively affected by existing tensions, conflict and instability, particularly in circumstances of war, insurrection and civil unrest.

The World Bank's ESS4 also addresses the health, safety, and security risks and impacts on project-affected communities and the corresponding responsibility of the client to avoid or minimize such risks and impacts, with particular attention to people who, because of their particular circumstances, may be vulnerable. When security personnel are used to provide security to safeguard project's personnel and property, there is a need to assess risks posed by these security arrangements to those within and outside the project sites. The sanctioning of any use of force by direct or contracted workers in providing security is discouraged except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.

### 2.1 National Polices and Legal Frameworks

#### 2.1.1 Provisions of the Constitution of Ethiopia

The Constitution of FDRE is the supreme law of the land. No law or customary practice or a decision of any organ of the state can contravene the Constitution. To this end, all citizens, organs of the state, political organizations, other associations as well as their officials have the duty to ensure the observance of the Constitution and to obey it. Additionally, the Constitution states all international agreements ratified by Ethiopia are an integral part of the law of the land. Therefore, any agreement related to the security, fundamental rights and freedoms that are ratified by the country are integral part of the law. The Constitution recognizes different rights of citizens as it relates to security of their persons. The following table summarizes some of those rights.

**Table 2—1. Relevant Constitutional Provisions-Ethiopia**

Constitutional Articles	Description of the Constitutional Right
<b>Article 14: Rights to life, the Security of Person and Liberty</b>	<ul style="list-style-type: none"> <li>■ Every person has the inviolable and inalienable right to life, the security of person and liberty.</li> </ul>
<b>Article 15: Right to Life</b>	<ul style="list-style-type: none"> <li>■ Every person has the right to life. No person may be deprived of his life except as a punishment for a serious criminal offence determined by law.</li> </ul>
<b>Article 16: The Right of the Security of Person</b>	<ul style="list-style-type: none"> <li>■ Everyone has the right to protection against bodily harm.</li> </ul>
<b>Article 17: Right to Liberty</b>	<ul style="list-style-type: none"> <li>■ No one shall be deprived of his or her liberty except on such grounds and in accordance with such procedure as are established by law.</li> <li>■ No person may be subjected to arbitrary arrest, and no person may be detained without a charge or conviction against him.</li> </ul>
<b>Article 18. Prohibition against inhuman Treatment</b>	<ul style="list-style-type: none"> <li>■ Everyone has the right to protection against cruel, inhuman or degrading treatment or punishment.</li> <li>■ No one shall be held in slavery or servitude. Trafficking in human beings for whatever purpose is prohibited.</li> <li>■ No one shall be required to perform forced or compulsory labour.</li> </ul>
<b>Article 19. The Right of Persons Arrested</b>	<ul style="list-style-type: none"> <li>■ Persons arrested have the right to be informed promptly, in a language they understand, of the reasons for their arrest and of any charge against them.</li> <li>■ Persons arrested have the right to remain silent. Upon arrest, they have the right to be informed promptly, in a language they understand that any statement they make may be used as evidence against them in court proceedings.</li> <li>■ Persons arrested have the right to be brought before a court within 48 hours of their arrest. Such time shall not include the time reasonably required for the journey from the place of arrest to the court. On appearing before a court, they have the right to be given prompt and specific explanation of the reasons for their arrest due to the alleged crime committed.</li> <li>■ All persons have an inalienable right to petition the court to order their physical release where the arresting police officer or the law enforcer fails to bring" them before a court within the prescribed time and to provide reasons for their arrest. Where the interest of justice requires, the court may order the arrested person to remain in custody or, when requested, remand him for a time strictly required to carry out the necessary investigation. In determining the additional time necessary for investigations, the court shall ensure that the responsible law enforcement authorities carry out the investigation respecting the arrested person's right to a speedy trial.</li> <li>■ Persons arrested shall not be compelled to make confessions or admissions which could be used in evidence or against them. Any evidence obtained under coercion shall not be admissible.</li> <li>■ Persons arrested have the right to be released on bail. In exceptional circumstances prescribed by law, the court may deny bail or demand adequate guarantee for the conditional release of the arrested person</li> </ul>

<p><b>Article 20. Rights of Persons Accused</b></p>	<ul style="list-style-type: none"> <li>■ Accused persons have the right to a public trial by an ordinary court of law within a reasonable time after having been charged. The court may hear cases in a closed session only with a view to protecting the right to privacy of the parties concerned, public morals and national security.</li> <li>■ Accused persons have the right to be informed with sufficient particulars of the charge brought against them and to be given the charge in writing.</li> <li>■ During proceedings accused persons have the right to be presumed innocent until proved guilty according to law and not to be compelled to testify against themselves.</li> <li>■ Accused persons have the right to full access to any evidence presented against them, to examine witnesses testifying against them, to adduce or to have evidence produced in their own defense, and to obtain the attendance of and: examination of witnesses on their behalf before the court.</li> <li>■ Accused persons have the right to be represented by legal counsel of their choice, and, if they do not have sufficient means to pay for it and miscarriage of justice would result, to be provided with legal representation at state expense.</li> <li>■ All persons have the right of appeal to the competent court against an order or a judgement of the court which first heard the case.</li> <li>■ They have the right to request for the assistance of an interpreter at state expense where the court proceedings are conducted in a language they do not understand.</li> </ul>
<p><b>Article 21. The Rights of Persons Held in Custody and Convicted Prisoners</b></p>	<ul style="list-style-type: none"> <li>■ All persons held in custody and persons imprisoned upon conviction and sentencing have the right to treatments respecting their human dignity.</li> <li>■ All persons shall have the opportunity to communicate with, and to be visited by, their spouses or partners, close relatives, friends, religious councilors, medical doctors and their legal counsel.</li> </ul>
<p><b>Article 25-Rights to Equality</b></p>	<ul style="list-style-type: none"> <li>■ All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall guarantee to all persons equal and effective protection without discrimination on grounds of race, nation, nationality, or other social origin, color, sex, language, religion, political or other opinion, property, birth or other status.</li> </ul>
<p><b>Article 35-Rights to Women</b></p>	<ul style="list-style-type: none"> <li>■ The historical legacy of inequality and discrimination suffered by women in Ethiopia taken into account, women, in order to remedy this legacy, are entitled to affirmative measures. The purpose of such measures shall be to provide special attention to women so as to enable them to compete and participate on the basis of equality with men in political, social and economic life as well as in public and private institutions.</li> <li>■ Women shall; in the enjoyment of rights and protections provided for by the Ethiopian Constitution, have equal right with men.</li> <li>■ Women have equal rights with men in marriage as prescribed by this Constitution.</li> <li>■ Women have the right to full consultation in the formulation of national development policies, the designing and execution of projects, and particularly in the case of projects affecting the interests of women.</li> <li>■ Women have the right to acquire, administer, control, use and transfer property. In particular, they have equal rights with men</li> </ul>

	<p>with respect to use, transfer, administration and control of land. They shall also enjoy equal treatment in the inheritance of property.</p> <ul style="list-style-type: none"> <li>■ Women shall have a right to equality in employment, promotion, pay, and the transfer of pension entitlements.</li> <li>■ The State shall enforce the right of women to eliminate the influences of harmful customs. Laws, customs and practices that oppress or cause bodily or mental harm to women are prohibited.</li> </ul>
<p><b>Article 42. Rights of Labor</b></p>	<ul style="list-style-type: none"> <li>■ Factory and service workers, farmers, farm labourers, other rural workers and government employees whose work compatibility allows for it and who are below a certain level of responsibility, have the right to form associations to improve their conditions of employment and economic well-being. This right includes the right to form trade unions and other associations to bargain collectively with employers or other organizations that affect their interest.</li> <li>■ Categories of persons referred to in paragraph (a) of this sub-article have the right to express grievances, including the right to strike.</li> <li>■ Government employees who enjoy the rights provided under paragraph (a) and (b) of this sub-article shall be determined by law.</li> <li>■ Women workers shall have the right to equal pay for equal work.</li> <li>■ Workers have the right to reasonable limitation of working hours, to rest, to leisure, to periodic leaves with pay, to remuneration for public holidays as well as healthy and safe work environment.</li> <li>■ Without prejudice to the rights recognized under sub-article 1 of this Article, laws enacted for the implementation of such rights shall establish procedures for the formation of trade unions and for the regulation of the collective bargaining process.</li> </ul>

### 2.1.2 Ethiopia's Labour Proclamation No. 1156/2019

Ethiopia's Labour Proclamation No.1156 of 2019, establishes the principles governing labour conditions in alignment with the country's constitutional, political, social, and economic policies and its commitments under international law. This law applies to employment relations based on a contract that exists between a worker and an employer including recruitment process. The law provides extensively for contractual relations, including the obligations of employers to protect the well-being of employees by ensuring safe working environments and reasonable working hours to prevent health risks and ensure their overall welfare.

In particular, Part Seven, Chapter One, and Article 92 of the Labour Proclamation specifically addresses occupational health and safety within the working environment and outlines the prevention measures and responsibilities of employers. Employers are mandated to ensure the well-being of workers by implementing necessary measures to safeguard their health and safety. Article 92 requires the employer to:

- Take appropriate steps to ensure that workers are properly instructed and notified concerning the hazards of their respective occupations; and assign safety officer; and establish occupational health and safety committee.

- Provide workers with protective equipment, clothing and other material and instruct them of their use.
- Register employment accidents and occupational diseases and report same to the labour inspection service.
- Arrange, according to the nature of work, at his own expense for the medical examination of newly employed workers and for those workers engaged in hazardous work, as may be necessary with the exception of HIV/AIDS unless otherwise the country has obligations under international law to do so.
- Ensure that the workplace and premises of the undertaking do not pose threats to the health and safety of workers.
- Take appropriate precautions to ensure that all processes of work in the undertaking shall not be a source or cause of physical, chemical, biological, ergonomic, and psychological hazards to the health and safety of the workers.
- Implement the instructions given by the competent authority in accordance with the proclamation.

Part Six, Chapter 1 and 2 of the Labour Proclamation No. 1156/2019 focuses on the safety of women and young employees. It cautions against assigning work to women that may endanger their health, including overnight or night shift work. It also prohibits workplace discrimination against women. Terminating a woman's employment during pregnancy and up to four months after childbirth is prohibited. Employers are required to grant leave to pregnant women without wage deductions and provide necessary occupational health and safety measures as outlined in the proclamation.

For young employees, the proclamation provides that employers are prohibited from hiring individuals under 15 years old. Those between 15 and 18 years should not work more than 7 hours per day, and they are further not allowed to engage in overnight shifts or night work. Moreover, the Occupational Health and Safety Directives sets limits on occupational exposure to conditions that could adversely affect their health and safety in the workplace.

### **2.1.3 Proclamation on Gender Based Violence and the Ethiopian National Policy on Women**

In addition to the constitutional provisions and the labour proclamation 1156/2019, there are other special provisions within the law that guarantees the security of women at the workplace. Of note is proclamation No.1097/2018 which identifies the elimination of Gender Based Violence in the workplace as a strategic priority. Article 28 bestows powers and to the responsible government ministry to “design strategies to effectively prevent and take measures against gender-based violence against women.”

The National Policy on women, which was issued in 1993, also emphasizes that all economic and social programs and activities should ensure equal access for both men and women to the country's resources and in the decision-making process so that women can benefit equally from all activities carried out by the Federal and Regional Institutions. Among the main policy objectives is that laws, regulations, systems, policies and development plans that are issued by the government should ensure the equality of men and women and that special emphasis should be given to the participation of rural women.

In addition, the National Policy on Empowerment of Women adopted in 2001 states that “All forms of violence against women, physical and mental, whether at domestic or societal levels, including those arising from customs, traditions or accepted practices shall be dealt with effectively with a view to eliminate its incidences. Institutions and mechanisms for assistance will be created and strengthened for prevention of such violence, including sexual harassment at workplace and customs like dowry; for the rehabilitation of the victims of violence and for taking effective action against the perpetrators of such violence. A special emphasis will also be laid on programs and measures to deal with trafficking in women and girls.”

Continuing the improvement of policy provisions, in 2005, the Women’s Affairs Ministry was established with a bid to coordinate women’s activities and translate the policy objectives. And, in 2006, the Ministry of Women’s Affairs issued the National Plan of Action for Gender Equality (NAPGE) for the period 2006-2010. Its goal is “to contribute to the attainment of equality between men and women in social, political and economic development.”

## **2.2 World Bank Environmental and Social Framework Requirement**

The Environmental and Social Framework recognize the need to assess and mitigate security risks and impacts. The need to address the assessment and mitigation of security related risks and impacts on project-affected communities and project workers is set out in Environmental and Social Standards (ESS) such as ESS1, ESS2, and ESS4, World Bank Group (WBG) Environment Health and Safety (EHS) Guidelines as well as the Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel and ISO 31000 (Risk Management Guidelines). Whenever, there are discrepancies between the national legislation and the relevant WB ESSs, WB ESS prevails. The applicable ESSs are discussed below:

### **2.2.1 ESS1: Assessment and Management of Environmental and Social Risks and Impacts**

This standard aims to identify, evaluate and manage the environment and social risks and impacts adopt a mitigation hierarchy approach Including avoidance , minimize or reduce risks and impacts to acceptable levels, utilize national environmental and social institutions, systems, laws, regulations and procedures in the assessment, development and implementation of projects, whenever appropriate and promote improved environmental and social performance, in ways which recognize and enhance Borrower capacity.

**Relevance:** “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.”

### **2.2.2 ESS2: Labor and Working Conditions**

ESS 2 focuses on the importance of employment creation and income generation in the pursuit of poverty reduction and inclusive economic growth. It requires the Borrower to promote sound worker-management relationships and enhance the development benefits of a project by treating workers in the project fairly and providing safe and healthy working conditions.

**Relevance:** The fact that the borrower is responsible to ensure health and safety of project workers. Moreover, to avoid or mitigate the potential security risks that may arise from workers discrimination, abuse, labour influx, unfair treatment, lack of equal opportunity etc.

### **2.2.3 ESS4: Community Health and Safety**

ESS4 recognizes that project activities, equipment design and safety, infrastructure, and safety services can increase community exposure to risks and impacts. It also addresses Infrastructure and equipment design and safety and safety of services which involves provision of services to communities and the corresponding responsibility of borrowers to avoid or minimize such risks and impacts. In particular, in conditions where the PMU engage direct or contracted workers to provide security to protect project workers and assets, ESS4 require to assess the risk posed by the security arrangements within and outside the project site. Besides, the standard states the PIU are expected to ensure that government security personnel deployed to give security services act guided by the principles of proportionality and GIIP, the WB Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel, and by applicable laws. Furthermore, the standard requires the PMU to verify and ensure the direct and contracted workers engaged to give security did not induce abuse. Moreover, ESS4 demands the PIU to review and take corrective measures for all accusations inappropriate doings of the security personnel.

**Relevance:** The security Risk Assessment and Management plan is mainly based on the ESS4. It requires borrower retaining direct or contracted workers to provide security to safeguard its personnel and property to assess risks posed by these security arrangements to those within and outside the project site. Besides, it seeks the borrower to ensure that government security personnel deployed to provide security services act in a manner consistent with the principles of proportionality and Good International Industrial Practices (GIIP), the WB Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel and by applicable law. The sanctioning of any use of force by direct or contracted workers in providing security is discouraged except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.

As set out in ESS4 Paragraph 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 program site. In making such arrangements, the Borrower will be guided by the principles of proportionality and Good International Industry Practice (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.

The provision in Paragraph 25 states that the Borrower will seek to ensure that government security personnel deployed to provide security services act in a manner consistent with Paragraph 24 indicated above and encourage the relevant authorities to disclose the security arrangements for the Borrower's facilities to the public, subject to overriding security concerns.

As per Paragraph 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 Environmental and Social Commitment Plan (ESCP).

Furthermore, as given in Paragraph 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 or abusive acts to relevant authorities.

#### **2.2.4 World Bank's Good Practice Note on Assessing and Managing Risks of the use of Security Personnel**

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 Program site. In making such arrangements, the Borrower will be guided by the principles of proportionality and Good International Practices, 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 of the threat.

The Borrower will seek to ensure that government security personnel deployed to provide security services act in a manner consistent with statements in the above paragraph and encourage relevant authorities to disclose the security arrangements for the Borrower's facilities to the public, subject to overriding security concerns. 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. 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 acts to relevant authorities." Decisions on the appropriate scope

of the Programs security arrangements are guided by an assessment of (a) potential risks to the Programs personnel and property, which may require a security response; (b) appropriate responses to the identified security risks; (c) potential impacts of a security incident on the Program, local communities, and other parties; and (d) potential mitigation measures.

The security arrangements for a Program may themselves pose risks to, and impacts on, Program workers and Local communities. It is important to take these risks and impacts into consideration and to determine measures to address them, and this should be part of the ongoing stakeholder engagement on the Program, as described in ESS10. Program-level grievance mechanisms that are available to Program workers, local communities, and other stakeholders allow them to provide feedback on the Program's security arrangements and personnel.

### **2.2.5 World Bank Group (WBG) Environment, Health and Safety (EHS) Guidelines**

WBG EHS Guidelines recognizes project workers and community risk of exposure to physical, chemical and other hazards related to the program activities. These risks may arise from intentional or unintentional trespassing, including potential contact with hazardous material handling and storage. It also suggests the need for prevention and mitigation of the risks through the implementation of project specific plans and relevant applicable management practices. Besides, the relevant Environment and Occupational, Health and Safety (OHS) standards recognize the risks related to construction which include noise and vibration, dust (affecting air quality), wastes, stuck by objects, dusts, work in height, fire and traffic safety risks etc. Moreover, the guideline requires and recognize the program to ensure availability of potable water for drinking, food preparation, for personal hygiene workers in the project site.

**Good Practice Note:** Assessing and Managing the Risks and Impacts of the Use of Security Personnel is provided by World Bank to accompany the ESF and ESSs to support its implementation. Accordingly, the Security Risk Assessment and Management Plan for FSRP is also based on the Good Practice Note.

## **2.3 International Standards and Good Practice**

There are also other international standards which could be referenced in the preparation, monitoring and implementation of Security Management Plan. Common to these Good International Practices they all emphasize that the use of security forces is based on the concept that providing security and respecting human rights can and should be consistent. This translates into implementation of policies and practices that ensure security provision is carried out responsibly, with any response being proportional to the threat. Proactive communication, community engagement, and grievance redress are central to this approach. Communications shall also often be performed through collaboration between security and community relations departments. Gender considerations are also important, as women often have different experiences and interactions with security personnel. The specific international standards and links for the full document are indicated below.

- 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
- Voluntary Principles (VPs) on Security and Human Rights
- <http://www.voluntaryprinciples.org/what-are-the-voluntary-principles>
- International Code of Conduct for Private Security Service Providers.  
[https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF-CONDUCT-Amended\\_2021.pdf](https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF-CONDUCT-Amended_2021.pdf)
- 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](https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces)

### **ISO 31000(Risk Management Guidelines**

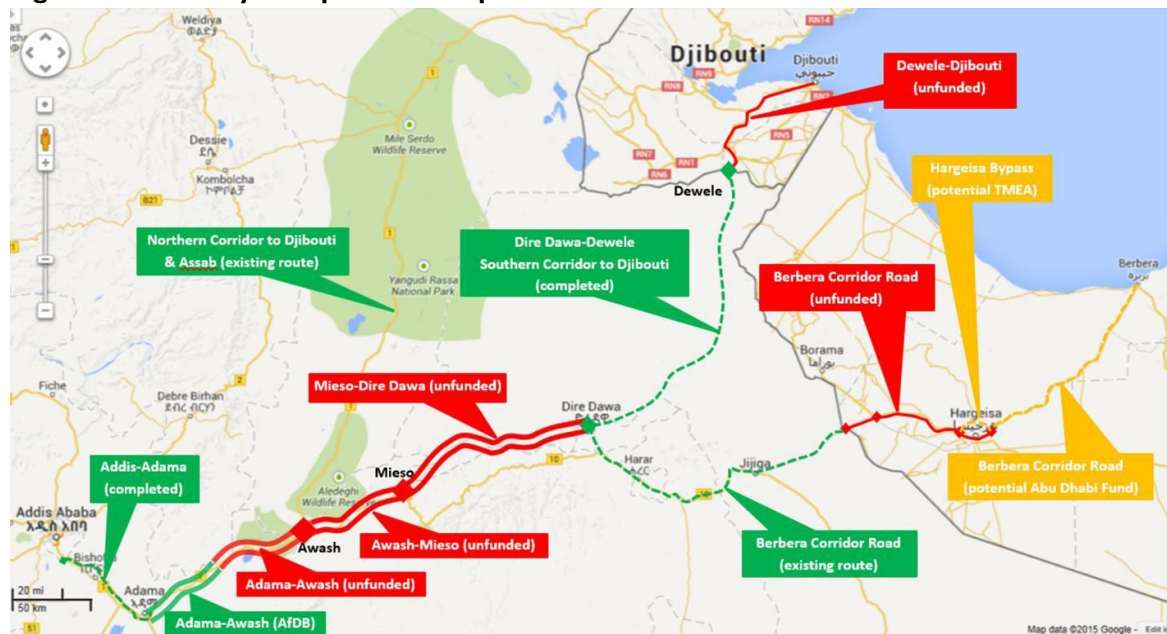
The ISO 31000 risk management is based on five principles include the requirement for the risk management initiatives to be customized, inclusive, structured and comprehensive, integrated and dynamic. It has risk management framework which is meant to assist with integrating risk management into all program management and activities. In addition, the risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. ISO 31000 recognizes the need for selecting the most appropriate risk treatment option(s) and designing risk treatment plan specifying how the options will be implemented. Furthermore, it emphasizes the need for monitoring and review the implementation. Above all, recording and reporting including communicating risk management activities and outcomes, providing information for decision making, improving risk management activities and providing risk information and interacting with stakeholders are the key components of ISO 31000.

# 3 SECURITY CONTEXT AND THREAT ASSESSMENT

## 3.1 National Security Context

Ethiopia, like other nations in the Horn of Africa, has faced inter-ethnic conflict, displacement, and drought over the past decades. The security situation has deteriorated in parts of the country since 2018 with militias and non-state actors responsible for the insecurity. The inter-ethnic clashes have caused death, the destruction of property, and large-scale displacement of people. As of 2023, reports indicate that there were 2.9 million internally displaced people in Ethiopia due to conflict and over 141,000 Ethiopian refugees and asylum seekers in neighboring countries. Due to the ethnic conflicts, the security situation in several parts of Ethiopia is volatile and unpredictable. Recently, violent clashes have occurred, especially in the Tigray Regional State, Amhara Regional State, and the northern areas of Afar Regional States bordering Tigray, southern parts of Somali regional State, Kelam Welega, East Wollega, Horo Guduru Welega, North Shewa, bale and Borena of the Oromia Regional State and Benishangul Gumuz Regional State. Between November 2020 and November 2022, armed conflicts took place in the northern regions of Ethiopia, in particular in Tigray but also in Amhara and Afar. The security situation along Ethiopia's border areas with neighboring countries is extremely unstable. Non-State armed groups including bandits, operate along Ethiopia's borders with Somalia, Sudan, South Sudan and Kenya. Inter-tribal clashes, including across national borders, and skirmishes between non-state armed groups and government forces are common in these areas. The risk of violent robbery and kidnapping in border areas is high. The terrorist group Al-Shabaab, based in Somalia, reportedly maintains a presence in areas close to the Ethiopian border. The transmission line traverses Somali region considered as volaties and borders borders Afar Regional state also considered a hotspot in terms of insecurity.

Figure 3-I. Security Hotspots in Ethiopia



Source: United Nations

## **3.2 Security Context in Transmission Line Project Route**

The SRA provides an overview understanding of the current situation across Ethiopia and in Somali Region from a political and security perspective. The main risks discussed in this report revolve around issues listed below.

- Political Instability
- Clan Conflicts
- Conflicts over pasture and water
- Flooding

### **3.2.1 Nature of Risks/Conflicts**

There is significant conflict at different levels in Ethiopia and specifically in Somali region. Some insecurity stems from clan competition, which goes back to historical movements and power distribution. The social impacts and potential aggravation of resource-related conflicts is well documented in a range of pastoralist and agro-pastoralist assessments carried out in the Somali region. Access to water and pasture is a fundamental source of both conflict and co-operation between clans and civil authorities throughout the the 2 regions. In terms of conflict, extensive trans-boundary movements of livestock and limited access to the combination of water and pasture is one of the primary drivers of conflict across the Horn of Africa and within Ethiopia. Long and well documented records of conflict and cooperation over access to water and pasture in pastoralism domain exist. Water points with adequate surrounding pasture are especially scarce, claimed by clans, fiercely guarded and intrinsically linked to resource conflict. Insecurity for women is still the number one issue that prevents gender equality and women's empowerment from being a feasible objective. Women continue to suffer disproportionately from clan-fights and extremist interventions.

## 4 SECURITY RISK ASSESSMENT

Risk assessment is a critical process that involves evaluating the likelihood of a risk occurring and the potential impact it would have if it does occur. It is essentially an assessment of a cause-and-effect relationship, where the “cause” is the event that could potentially occur, and the “effect” is the impact the event would have on various aspects of a construction project, including impact on workers, local communities, and other stakeholders.

The recognition, mitigation, and communication of security risks and hazards associated with the project is a critical element of this SMP to help achieve the goal of limiting security risks and instances in the project implementation. Risk assessment allows a project to identify, analyze, and prioritize risks to implement effective mitigation strategies and minimize potential negative outcomes.

Security risks assessment was conducted to establish, implement, and maintain a documented risk assessment process for the risk identification analysis, and evaluation of the proposed project in order to:

- Identify potential security risks due to intentional and unintentional threats that have a potential for direct or indirect consequences on the proposed electricity project activities, assets, individual workers, community, and other stakeholders.
- Systematically analyze potential risks (its likelihood and consequence analysis).
- Determine those potential risks that have significant adverse impact on the activities of the proposed electricity project, contractors, subcontractors, assets, workforce, and local communities.
- Determine those potential risks that have significant adverse impact on the environment (flora and fauna).
- Systematically evaluate and prioritize security risks controls and mitigation measures.

Therefore, the project shall:

- Document and keep this SMP and update it during project implementation.
- Periodically review the SMP during project implementation and reassess whether the prior assessments are still appropriate.
- Re-evaluate security risks within the context of changes within the contractor’s working environment and relationship with local communities.
- Ensure that the prioritized security risks and impacts are taken into consideration in establishing and implementing this SMP.

### 4.1 Methodology of the Security Risk Assessment

To prepare this SMP, the project relied on both primary and secondary data for its review. In conducting secondary data review, the SMP reviewed international, national and regional legal instruments and legislation and other regulations such as the Good International Industrial Practices (GIIP), ISO 31000(Risk Management Guidelines), the World Bank’s Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel, and the United Nations Security Management System

(UNSMU). Additionally, research findings on the country's security situation were also reviewed and utilized. The primary data collections methods employed by the project included observation of selected target project corridors, interviews with community members including local leaders and elders, observations and consultation sessions with local police and security forces and other project stakeholders.

- **Visual Observations:** The project relied on conducting a visual observation of certain areas in the target project corridor. The observation involved walking through the mapped project area and noting and recording incidents that raise potential security concerns.
- **Interviews:** The project also conducted interviews. Interviews are an effective primary tool for gaining information related to potential security risk and impacts related to the project. Focused interviews were conducted with different community representatives, government officials, and focal persons. The interviews collected information on potential security risk or impacts, the likelihood of the risks to occur, potential security responses, the severity of the risks and impacts, on security incidents and potential responses, including potential mitigation measures.
- **Consultations:** Consultations with different stakeholders was also done. Consultations were conducted with community representatives, local and regional police forces, and local leaders, to discuss and map the potential security risks and impacts, relationships of security personnel with the community, the likelihood and severity of the security risks and the impacts of such risks on the community, as well as other security issues that affect the communities.

## 4.2 Objectives of Assessing Security Risks

The following are the main objectives of potential security risk assessment for the project:

- Identify, evaluate, and prioritize risks and likely security responses.
- Understand and respond to community concerns and perceptions.
- Determine appropriate security arrangements.
- Propose mitigation plans and develop implementation strategy.
- Set, monitor, and audit strategies of implementation of SMP.

## 4.3 Risk Assessment Approaches

During the potential risk assessment of the proposed electricity project corridor, the following methods and approaches were followed:

- a) Security Risk Trend Assessment Approach
- b) Current Security Condition Assessment.

### 4.3.1 Security Risk Trend Assessment

Trend assessment plays a crucial role in understanding security risks and changes over time. In addition to the potential security risks assessed during the Environmental and Social Impact Assessment (ESIA), a security trend assessment that reviewed five years of security situations along the project covered corridor was carried out. This assessment provided valuable insights into past security risks and how they may inform the present circumstances. This assessment involved community consultations, interviews with key

stakeholders at regional, zonal and district levels, and an analysis of secondary data. The security trend assessment aimed to:

- Capture historical security risks in the areas where the electricity project is planned.
- Determine the current security situation compared to the past.
- Identify the local communities where security threats have been recurring, posing risks to the project and workers.
- Understand how local communities have dealt with these threats in the past and what has been successful.
- Assess potential risks arising from inadequate security management, both internally and externally.

### 4.3.2 Current Security Condition Assessment

The current security conditions along the proposed project area were assessed as part of the ESIA, which includes the SMP. This assessment involved several methods:

1. **Site observation:** direct observation of the electricity project corridor was done to evaluate the current security situation.
2. **Interviews:** Interviews were conducted with various stakeholders, including communities living in the area, religious leaders, local elders, government security bodies such as the police, and relevant government ministries. These interviews aimed to gather insights and perspectives on the existing security conditions.

## 4.4 Security Risk Identification

Projected Security risks for the electricity project can be categorized as follows:

1. Internal security risks
2. External security risks

### 4.4.1 Internal Security Risks

Internal security risks are risks that are primarily driven by the unauthorized, unethical, or improper actions of project construction personnel and affiliated individuals, including suppliers of construction materials and services. Some common internal security risks that may arise in the implementation of the electricity project include:

- **Employee theft**-unauthorized taking of project resources, materials, or equipment by project personnel.
- **Conflicts caused by disrespect of local cultures or beliefs**-Incidences where workers' actions or behaviors disrespects the local community's culture and beliefs, potentially leading to conflicts between workers and local communities.
- **Workplace violence and labour unrest** -Instances of violence or unrest within the workplace, which may escalate to sabotage or disruptions in project operations.
- **Inappropriate Security Personnel Response**-Harsh or illegal responses by security personnel, leading to fear, distrust and conflict among employees at the workplace or other individuals involved in the project.

These internal security risks can pose significant threats to the project and to the safety and well-being of workers, and the relationship between the project team and the local community. Proactive measures and effective security protocols are essential to mitigate

these risks and ensure a secure and harmonious work environment for all stakeholders involved in the project.

#### **4.4.2 External Security Risks**

External security threats are those threats driven by individuals or groups external to the project who exploit opportunities arising from the project's activities to achieve various objectives. They include common criminal activity, disruption of the project activities for political, social or economic gain, and other deliberate actions that negatively impact the project's effectiveness and safety, leading to potential risks and challenges in project execution. Some common external threats include:

- Theft of equipment and material from project sites or individual houses
- Burglary committed by external individuals.
- Banditry or roadside attacks targeting workers during transit of equipment and material to project sites.
- Community unrest due to various factors like labour influx, improper behaviors, conflicts over land and water use, and environmental issues.
- Gender based violence and sexual exploitation affecting women and girls in project areas, posing a security concern.
- Risks arising from the use of security personnel, potentially exacerbating tensions with the local communities.
- Risk of traffic accidents due to higher traffic flow, and unsafe driving as well as bad roads.
- Risks associated with armed conflicts, including government and non-government forces, and the potential threat of staff kidnapping.
- Medical risks due to limited access to medical care in remote or rural areas.
- Exposure to natural hazards like flooding during rainy seasons, posing risks to the project personnel.

### **4.5 Data Collection Main Findings**

The consultations, interviews and observations revealed the following information:

#### **The project does not pose any significant risk to the communities.**

As to whether the project poses a security risk to the benefitting communities, the findings from the interviews, consultations and visual observations, revealed that the project does not pose any noteworthy security risk. Rather, there was unanimity of opinion that the project would only bring benefits to the target communities by improving the infrastructure and standards of living. Nevertheless, there are some situations which if not managed correctly, may result in mistrust between the project and the community which may in turn lead to future security problems. Such instances include occasions of unmet expectations related to the program by the community, access restriction, land acquisition without adequate consultation and compensation, trespassing and labour influx.

#### **Nature of security to be provided and personnel responsible**

The consultations revealed that the best way to provide security is to use local security members from the communities who have the same background and a sense of belonging as the community. The people applying to be security personnel should meet the

recommendations of the local officials and elders. The recommendations should be based on the prior discipline records, community involvement, experiences and relationships within the community.

### **Potential Impact of Major Security Incidents to the Project**

Serious Security incidences such as armed conflicts and community unrest could lead to devastating effect to the project and the project workers. Such kind of insecurity could potentially result in injuries and even death to project workers and could extensively damage property. In the event of such conflict, workers would need to be temporarily evacuated, and project could be disrupted for an extended time.

### **Possible Mitigation Measures**

The consultations and interviews revealed that security assessment, communication and disclosure of the security situation of each project site at the planning stage and throughout implementation, is key to a proper security response. The need to enact physical measures to prevent access to construction sites through putting in place fences, gates, and hiring of guards was stressed. In addition, working closely and maintaining regular communication with security actors was viewed as key to a proper security response. Continued consultation and involvement of key stakeholders, project workers, community members and program affected people in all project activities would help to avoid or mitigate security issues that might happen in relation to the program activities and unmet expectations related to the program. Moreover, provision of priority in employment opportunities created by the program subprojects would help create good relationship with the community through avoiding or minimizing the potential security issues that may happen due to labour influx.

## **4.6 Main Security Threats**

The SMP revealed certain main findings in regard to potential security threats involving the project. In its review and analysis, the project categorized the potential security risks as either internal or external.

- **Internal security threats:** - security threats that stem from workers within the project or incidents that occur in the workplace. Internal threats may involve issues like theft, sabotage, equipment damage, labour disputes, and conflicts among the workers.
- **External security threats:** - security threats that originate from outside the project and involve risks posed by individuals or groups aiming to exploit vulnerabilities in the project. External threats include thefts of project equipment, physical threats and harm to workers, vandalism, and disruption of the project for economic, political or social reasons.

The SMP revealed that the potential magnitude and scope of security issues varies from theft, burglary and roadside attacks on workers during transit, to armed conflicts, natural disasters such as flooding, Gender Based Violence (GBV) and sexual abuse. Based on findings from the security risk assessment, the following inexhaustive list constitutes the identified potential security threats from the project:

Accordingly, based on the assessment conducted, some of the potential security risks to project may include the following:

- **Theft of equipment and material:** employee or visitor/guest stealing equipment or material from project site or individual house.
- **Burglary:** Illegal entry of a building with intent to commit a crime, especially theft. It involves breaking and entering the premises. This can be done by staff or outsiders.
- **Banditry/Roadside attacks on workers during transit:** The project can be susceptible to attacks while transporting equipment and materials to the targeted regions or to project workers when travelling for field activities.
- **Community unrest:** Due to influx of labor, improper behavior towards the community, land and water use conflict, improper site selection and locating project infrastructures and associated facilities, resource abuse by the contractors, improper waste disposal, noise and dust pollution, etc.,
- **Risks from Employee industrial action and disruption of services:** Likely cause for labor disputes include demand for limited employment opportunities; labor wages/rates and delays of payment; disagreement over working conditions, raising concerns regarding unsafe or unhealthy work situations, or any grievances raised, and such situations could lead to labor unrest and work stoppage.
- **Gender-based violence (GBV)/sexual exploitation and abuse (SEA) and gender-based security incidents:** This becomes a security issue when GBV/SEA is inflicted by perpetrators to women and girls of the project workers and community in the project area (For more detail assessment on GBV risks, please refer GBV Action Plan Annex).
- **Risks emanating from the use of security personnel:** Use of security personnel may exacerbate tensions. Security personnel can be private or public. Security personnel can be engaged by the project contractor. Their presence can pose risks to, and have unintended impacts on, both project workers and local communities. Examples include committing a GBV/SEA act by security personnel within conflict affected work environment. It can also occur during community unrest and actions ethnic conflicts within the work environment.
- **Risks associated with armed conflict and kidnapping: armed conflict between government and non-government forces** and between non-government armed forces. In areas in which armed groups are operating, there are risk of staff kidnapping.
- **Environment and OHS risks:** Program activities pose potential Environment and Occupational, Health and Safety (OHS) risks which include exposure to hazardous material, noise and vibration, dust (affecting air quality), wastes, stuck by objects, work in height, fire and risks associated with availability of potable etc.
- **Risk of traffic accident:** due to erratic driving habits and poorly maintained road infrastructure traffic accidents are potential risks.
- **Medical risk:** Access to adequate medical and emergency care in rural areas of the country is limited causing medical risks.
- **Exposure to natural hazard (flooding):** the rainy season in Ethiopia runs from June to September, and during this period flooding is common posing flooding.

## Threat Scenario

Threat Scenarios that are prevalent across the country as mapped out in the threat map revolve around threats to; Infrastructure; to Movement, to Worksite and Local Population and workers listed below. Table 4-2 presents nature of threat to the groups identified above.

**Table 4—1. Category of Workers**

Category of Workers	
Affected Persons	Definition
<b>Direct Workers</b>	People employed directly by the EEP-PIU, EAPP-PIU to work specifically in relation with the Project including staff of the PIU.
<b>Contracted Workers.</b>	People engaged through third parties to perform work on the project, regardless of location.
<b>Project-Affected Person</b>	This group includes anyone who is affected by the project in any way and could be put in harm's way through project activities. This can be, for example, a beneficiary.

**Table 4—2. Threat Scenarios**

Target	Nature of Threat
Threat to Infrastructure- These are permanent structures that are related to Project staff (i.e. offices, compounds, government buildings, hotels, etc.)	<ul style="list-style-type: none"> <li>• Vehicle Born Improvised Explosive Devices (VBIED) Person Born Improvised Explosive Devices (PBIED) Improvised Explosive Devices (IED)</li> <li>• Hand Grenade Attack</li> <li>• Rocket-Propelled Grenade (RPG) Attack</li> <li>• Indirect Fire Attack Civil Unrest Shooting</li> <li>• Armed Robbery/Raid Sabotage</li> <li>• Intimidation or Extortion Workplace Violence</li> <li>• GBV</li> <li>• Arson</li> <li>• Illegal blockade or occupation of infrastructure by hostile protestors</li> <li>• Compound takeover or hostage taking by hostile elements</li> <li>• Kidnapping</li> </ul>
<b>Threat to Movement-</b> These are any moves conducted by anyone on project business	VBIED PBIED IED <ul style="list-style-type: none"> <li>• RPG Attack</li> <li>• Complex Attack/Ambush Indirect Fire Attack</li> <li>• Civil Unrest Shooting Hijack</li> <li>• Running Attack GBV</li> <li>• Kidnapping</li> </ul>
<b>Threat to Worksite-</b> Semi permanent locations, utilised for a defined period of time whilst project works are ongoing	<ul style="list-style-type: none"> <li>• VBIED PBIED IED</li> <li>• Hand Grenade Attack Complex Attack Indirect Fire Attack Civil Unrest</li> <li>• Shooting</li> <li>• Armed Robbery/Raid Sabotage</li> <li>• Intimidation or Extortion Workplace Violence</li> <li>• GBV</li> <li>• Arson</li> <li>• Illegal Blockade/Occupation of infrastructure by hostile protestors</li> <li>• Compound Takeover/Hostage Taking by hostile elements</li> <li>• Kidnapping</li> </ul>
<b>Threat to Local Population</b> - Any local population whose security	<ul style="list-style-type: none"> <li>• Complex Attack Indirect Fire Attack IED</li> <li>• Hand Grenade Attack Bombing</li> <li>• Intimidation or Extortion GBV</li> </ul>

is adversely affected by the presence of project activity	<ul style="list-style-type: none"> <li>• Civil Unrest</li> </ul>
---	--

## 4.7 Security Risk Analysis and Evaluation

Likelihood of these risks will occur

Based on current situation and historical context, the likelihood of occurrence of the above-mentioned security risks will be assessed below. Accordingly, for the purpose of this document the Likelihood of occurrence of risk is measured on scale ranging from 1 (very unlikely) to 5 (very likely).

**Table 4—3. Likelihood of Risk Occurrence**

Likelihood	Description	Rating
Very likely	Will undoubtedly happen/recur, possibly frequently	5
Likely	Will probably happen/recur, but is not a persisting issue/circumstances	4
Moderately likely	Might happen or recur occasionally	3
Unlikely	Not expected to happen/recur but it is possible it may do so	2
Very unlikely	This will probably never happen/recur	1

The subsequent impact of the risks is measured on 1 to 5 scale from Negligible, Minor, Moderate, Severe and Critical.

**Table 4—4. Risk Severity descriptions and rating**

Severity	Description/ potential Trigger	Rating
Critical	<ul style="list-style-type: none"> <li>■ Critical unrest/conflict in neighboring impacting on project activities</li> <li>■ Staff kidnapping due to armed conflict around project operating areas</li> <li>■ Ongoing operations are unsustainable, and projects may be suspended for indefinite periods</li> <li>■ Death or severe injury of team member.</li> <li>■ Withdrawal/lack Govt support to ensure security.</li> <li>■ Destruction or total loss of assets</li> </ul>	5
Severe	<ul style="list-style-type: none"> <li>■ Only essential operational travel should be considered Management Unit</li> <li>■ Severe costs to the programme major disruption of activities</li> <li>■ Conflict is high</li> <li>■ Projects may be suspended at short notice</li> <li>■ Serious injury and possible death to project personnel</li> <li>■ Armed conflict in the project vicinity seriously impacting project activities</li> <li>■ GBV/SEA/SH risks</li> </ul>	4
Moderate	<ul style="list-style-type: none"> <li>■ Community unrest risks;</li> <li>■ Temporary program delays;</li> <li>■ Non-life-threatening injury to project personnel;</li> <li>■ Loss or damage to assets;</li> </ul>	3

Minor	<ul style="list-style-type: none"> <li>Limited conflict between local community and labor from other area with minor impact on the project;</li> </ul>	2
-------	--	---

In these context, Security Risk Management is the process of identifying future harmful events (“threats”) that may affect the achievement of project objectives. It involves assessing the likelihood and impact of these threats to determine the assessed level of risk to project and identifying an appropriate response. Security risks are controlled through prevention (lowering the likelihood) and mitigation (lowering the impact). Hence, risk is the combination of the likelihood of a threat being carried out and the subsequent impact. And it is calculated as

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

According to the UN Security Management System (UNSMS) security risk model (SRM) model first separately rate the likelihood and impact on 1-5 scale and combined to indicate the risk level each potential incident carries for the program operation. The risk score range and respective risk level a potential incident is shown in the Risk matrix below:

**Table 4—5. Risk Matrix and Score Range**

Risk score range	Risk level	<b>Action to be taken</b>
1 to 5	Low	Operations continue, security risks monitored regularly
6-10	Medium	Operations continue with heightened monitoring of security risks
11-15	High	Operations continue with intensive monitoring of security risk and immediate response to the risks
16-20	Very High	Operations continue, once control measures to reduce security risk to As low as Reasonably Practicable (ALARP) are introduced, etc.).
21-25	Unacceptable	

**Table 4—6. Security Risk Identified**

Security Risk Identified	Gebiley	Hargeisa	Berbera
Burglary and theft of equipment and materials	4	4	4
Banditry/roadside attacks on workers during transit	9	9	6
Community unrest	6	6	6
Risk from employee industrial action	4	4	4
Gender-based violence/sexual exploitation and abuse (SEA):	12	12	12
Risks emanating from the use of security personnel	4	4	4

Risks associated with armed conflict and kidnapping	12	8	8
Environment and OHS risks	8	8	8
Exposure to natural hazard (flooding)	8	8	8
Risk of traffic accident	4	4	4
Medical risk	6	6	6

# 5 SECURITY RISK PREVENTION AND MITIGATION

## 5.1 Approach to Managing Security Risk

### 5.1.1 Development of the Approach

To balance (i) the need to support development benefits with (ii) managing the significant security risks, the project attempts a threefold approach:

- Screening out extremely high-risk areas, with a phased approach allowing reassessments and potential integration of areas where the situation improves over time;
- Risk management measures for moderate to substantial risk areas which remain volatile.
- Measures to scale down and or delay interventions in volatile areas with increasing risks informed by reassessments.

### 5.1.2 Phased Approach

The following phased approach in managing security risks is proposed

- Site-specific assessments in the regions will be required prior to the commencement of the infrastructure works through support from security risk management firms;
- Only for acceptable risk levels, a no objection to commence works for specific sites will be provided by the Bank.
- Further protocol details and holding point structures will be included in the Project Operation Manual. This will include a procedure to include management views on World Bank no objection to launch new phases of network deployment or initiating contracts in previously higher risk areas.

### 5.1.3 Additional Measures

Further additional measures are provided below.

- For areas where works are at acceptable risk level, basic risk management approaches will be outlined in the site-specific Security Management Plans (SMP).
- Training workers on-site on basic security elements, response to and reporting incidents among other will also be undertaken.
- In addition, capacity strengthening measures including security advisors in the PIUs will be required from the client
- The task team will work with procurement to ensure flexibility in contracting and budgeting in need for a ‘security premium’ for contractors who will hire additional security; while a militarized approach to security will be avoided.
- Specialized security risk management firms will be hired to support assessments as needed.

### 5.1.4 Adaptation and Monitoring

- Adaptation and Management will be undertaken as detailed below.
- While security risks are likely to continue to be high throughout the project implementation period, they are also dynamic. There could be a possibility of

requiring suspension of or limiting project activities until permissible conditions are achieved in areas with high risk.

- Similarly, in areas with low risks, activities are expected to proceed with continuous review of the risk situation and implementation. Flexibility will be built into contracting to allow for a stop-start approach if the threat profile changes.
- Local site-specific assessments and evaluation of potential security risks will help in determining the level and types of security arrangements required to be put in place. The SMP will outline a tier approach to assessments to reduce the required number of reiterations for detailed site assessments.
- Use of third-party monitoring agents to provide independent assessments and reassessments of the evolving security risk profile and the adequacy of risk mitigation measures deployed.
- Local SMPs are available and included in bidding documents.
- Security will not be used as a competitive element in the bidding process, beyond ensuring that the contractor has minimal qualifications including an appropriate security track-record.
- The contractors will not cut back on security measures without PIU endorsement

### **5.1.5 Security Risks Mitigation Measures**

For all threat scenarios that are detected in any local SRA a suite of risk mitigation measures will be identified specific to that threat scenario. For each Risk Level (STOP, Extreme, Substantial, Partial and Low) a proportionate amount of these risk mitigation measures will be assigned to the threat scenario. Contractors will be informed during the tender process of the perceived threat scenarios to their specific project activity, the risk level of each threat scenario for each category of worker and the required risk mitigation measures they are obligated to implement. In this manner Contractors can cost for the required risk mitigation measures as part of the tender process. It may be that a variety of risk mitigation measures can be used to effectively mitigate the risk and in this case the implementing partner will be given the choice of which mitigation measures to enact.

A full list of all threat scenarios, with their risk scores/risk levels and required risk mitigation strategies will be found in the Local Security Management plan. Contractors prior to commencing project activity, will be required to produce an Activity Security Plan (ASP). In this plan they will pick from the local SMP all threat scenarios that are relevant to their project activity and articulate via the ASP template which of the proscribed risk mitigation measures they intend to implement. This plan will be presented for sign off to the PIU Security Officer. Table 5-1 below table lists the potential security risks and potential mitigation measures.

**Table 5—1. Operational Health and Safety Risks and Mitigation Measures**

Potential Security Risk	Magnitude of Risk	Mitigation Measures
Thefts including theft of project equipment	Medium to High	<ul style="list-style-type: none"> <li>■ Implementing access control systems to secure and monitor entrance and outlet points of the workplace, proper badge and visitor card system, etc.</li> <li>■ Ensuring that visitors are never left unaccompanied in the workplace.</li> <li>■ Ensuring proper security lighting</li> <li>■ Where necessary, recruit and retain trained security guards.</li> <li>■ Maintain a properly executed inventory system.</li> <li>■ Minimize the amount of valuables and cash carried.</li> <li>■ Seek advice from local staff as to local areas considered insecure.</li> <li>■ Train and aware project workers on security plan and context of the area.</li> </ul>
Burglary and Vandalism	Medium to High	<ul style="list-style-type: none"> <li>■ Maintenance and up-grading of access control and surveillance systems.</li> <li>■ Install security lights to ensure visibility camps, facilities and material storage areas.</li> <li>■ Ensure proper fencing that is responsive to different security contexts.</li> <li>■ Have full time security personnel at the facilities and camp site.</li> <li>■ Establish formal and consistent reporting and communications mechanisms with public security forces and other stakeholders.</li> <li>■ Train and aware project workers on security plan and context of the area</li> </ul>
Clashes and conflicts within the work environment	Medium to High	<ul style="list-style-type: none"> <li>■ Conduct regular trainings and security awareness programs for project workers.</li> <li>■ Ensure functionality of grievance redress mechanism.</li> <li>■ Adhere to the Labour Management Procedure</li> <li>■ Conduct regular meetings with staff members.</li> </ul>
Community Unrest	Medium to High	<ul style="list-style-type: none"> <li>■ Provide awareness creation on precautionary measures need to be taken during community unrest.</li> <li>■ Ensure operational grievance management procedure that communities can use to raise their dissatisfaction and ensure that community concerns are addressed in a timely manner.</li> <li>■ Undertake stakeholder engagement and community dialogues to get the views and concerns of communities as per the stakeholder engagement plan.</li> <li>■ Increased vigilance should be implemented during periods of community unrest (avoid all large public crowds, including political gatherings and peaceful protests</li> <li>■ Any event having a potential to change the security situation within the operational areas must be communicated to management so that appropriate steps can be taken.</li> </ul>
Gender Based Violence	Medium to High	<ul style="list-style-type: none"> <li>■ Train security personnel on the project’s Code of Conduct (CoC) and ensure that contracted security personnel sign the CoC.</li> </ul>

		<ul style="list-style-type: none"> <li>■ Strengthen the treatment and referral pathways for GBV/SEA survivors.</li> <li>■ Raise awareness on GBV/SEA protocols for the project in line with the Labour Management Plan.</li> <li>■ Provide separate washrooms and bathrooms for men and women at the workplace.</li> <li>■ Ensure proper lighting at the worksite.</li> </ul>
Risks arising from the use of security personnel	Medium to High	<p>The project will be guided by the National Laws while addressing security concerns. The World Bank's ESF provides for possible mitigation measures for security personnel engaged in WB financed projects which include the following:</p> <ul style="list-style-type: none"> <li>■ Monitor risks resulting from acts of security personnel.</li> <li>■ Make reasonable inquiries to verify that the direct or contracted workers providing security are not implicated in past abuses.</li> <li>■ Raise awareness to contracted security personnel or determine that they are properly trained in the use of force and appropriate conduct towards workers and affected communities.</li> <li>■ Review allegations of unlawful or abusive acts of security personnel</li> <li>■ Ensure security personnel contracted under the project are inducted on and sign the CoC</li> <li>■ MoU will be signed (where applicable).</li> </ul>
Insecurity during transit	Medium to High	<p>There is risk of project and personal vehicles being attacked while in transit. This can be mitigated by:</p> <ul style="list-style-type: none"> <li>■ Obtaining prior intelligence information regarding vulnerable routes and avoiding travel during certain times.</li> <li>■ All project workers and visitors must have the appropriate security clearance and information before undertaking any travel.</li> <li>■ Transport goods and workers during the day to reduce the risk of attack.</li> <li>■ Ensure travelers have backup food, water, communication apparatuses (e.g. mobile phone), etc.</li> </ul>
Risks relating to armed conflict including kidnappings	Medium to High	<p>Risks relate to armed conflicts.</p> <ul style="list-style-type: none"> <li>■ Ensure good contacts with national law enforcement agencies, with a view to obtaining the best possible protection for project workers.</li> <li>■ Ensure up-to-date, detailed instructions project workers on security situations and precautions they should take in relation to the implementation of the security plan, including a comprehensive listing of emergency supplies they should have on hand and guidance on their behavior during a variety of emergencies, including armed conflict.</li> <li>■ Project workers should familiarize themselves with information provided to them regarding the security management system at their location.</li> <li>■ keeping the federal and regional Program Manger informed, on Safety and Security, of all developments in the subproject area which might have a bearing on the security and</li> </ul>

		<p>protection of the staff project workers for decision.</p> <ul style="list-style-type: none"> <li>■ Project leaders at all levels should ensure that staff members are acquainted with existing or potential security problems in the areas which they intend to visit and that they have obtained necessary security clearance before travelling.</li> <li>■ Train and aware project workers on security management plan and security context of the subproject area.</li> <li>■ Report incidents related to armed conflict.</li> </ul> <p>Risks related to kidnapping.</p> <ul style="list-style-type: none"> <li>■ Use of physical security personnel.</li> <li>■ Ensure consistent reporting and communications mechanisms with public security forces and other stakeholders.</li> <li>■ Staff should avoid travel in darkness; only using trusted drivers.</li> <li>■ Drivers should not set patterns and routines and should keep in pairs or teams at all times.</li> <li>■ Local knowledge of the program/subproject area and operational context must be maintained by staff at all times.</li> <li>■ Seek information from project security focal person and clearance before travel.</li> <li>■ Any event having a potential to change the security situation within program areas must always be communicated to the project and security coordinators so that appropriate steps can be taken.</li> <li>■ The Security Management Plan should be made available to all staff and appropriate training conducted.</li> <li>■ Never fight back when apprehended with armed people.</li> <li>■ Do not try to argue or make provocative comments.</li> <li>■ Do not stare or make eye contact with kidnapers.</li> </ul>
Environment and Occupational Health and Safety Risks	Medium to High	<ul style="list-style-type: none"> <li>■ Conduct regular training and awareness program ESMF, LMP, ESHS Guidelines, OHS, safety hazards, programs for project workers, community and IAs.</li> <li>■ Environmental and Social Clauses for Contractors Consultation</li> <li>■ Adhere to Hazardous material and Wastes Management set out in the ESMF.</li> <li>■ Adhere to Labor Management Procedure.</li> <li>■ Adhere to Liquid and Solid Waste Management Guideline prepared for FSRP.</li> <li>■ Ensure ESHS/OHS provisions are incorporated in the bidding documents and contract agreement for construction.</li> <li>■ Ensure that waste management is operable to reduce the fuel element for fire.</li> <li>■ Ensure a fire alarm/smoke alarm system is operable within the Agricultural research centers.</li> <li>■ Conduct regular Environmental and Social Monitoring and audit.</li> </ul>

		<ul style="list-style-type: none"> <li>■ Conduct regular emergency drills at project sites in coordination with relevant local authorities.</li> <li>■ Promptly report incidents related to OHS.</li> </ul>
Exposure to Natural Hazards such as flooding	Medium to High	<ul style="list-style-type: none"> <li>■ Be situationally aware of flood zones and of workers located in such areas.</li> <li>■ Get out of low areas subject to flooding during raining.</li> <li>■ Evacuate immediately to high ground if you think you are at risk or are advised to.</li> <li>■ Never try to walk or swim through flowing water.</li> <li>■ Be aware of flash flood areas such as canals, streams, drainage channels.</li> <li>■ Wait until it is safe to return.</li> <li>■ Monitor weather channels before, during and after flooding.</li> </ul>
Risk of Traffic Accidents	Medium to High	<ul style="list-style-type: none"> <li>■ Properly implement road traffic assessment and management plan prepared for the SMP</li> <li>■ Vehicles should be serviced and well maintained.</li> <li>■ Staff should be briefed on what to look for when hiring a vehicle in a remote location.</li> <li>■ Training of drivers in advanced First Aid should be a priority.</li> <li>■ Hire or train drivers on changing of essential parts of vehicles if required.</li> </ul>
Medical Risk	Medium to High	<ul style="list-style-type: none"> <li>■ Project workers should be trained on basic first Aid.</li> <li>■ First Aid packs must be availed to the site and field visit.</li> <li>■ The team has ascertained availability of emergency services in case of medical emergency.</li> <li>■ Persons carrying medications have more than enough for the whole trip and appropriate storage means.</li> <li>■ The team has self-disclosed to fellow team members relevant medical conditions / history in event unable to recount details themselves.</li> <li>■ Records / letters with history / medication in local language are being carried.</li> </ul>

## 6 SECURITY APPROACH

To ensure security EAPP-PIU/EEP-PIU will work with all relevant stakeholder within and across institution or organization. In this regard, 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. Dialogue with communities about security issues can help to identify potential risks and local concerns and can serve as an early warning system.

Besides, EAPP-PIU/EEP-PIU and Contractors shall communicate their security arrangements to workers and communities, subject to overriding safety and security needs. In addition, community members should be aware of their ability to make complaints without fear of intimidation or retaliation. Because security personnel 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.

Furthermore, grievance redress mechanism shall be established in the government devolving structure which will village, district and regional level. Moreover, the World Bank grievance redressing services are also available. The project-level grievance mechanism shall accept concerns or complaints regarding the conduct of security personnel and that such concerns and complaints, as well as any associated evidence and facts, be promptly documented and assessed and action be taken to prevent recurrence. The responses implemented in response to complaints are monitored and the outcomes communicated to relevant parties, taking into account the need to protect the confidentiality of victims and complainants. Besides, the establishment of functional and accessible Grievance Redress Mechanism (GRMs) would help to reduce the risk of community members resorting for protest and roadblock to draw attention to their grievance in situation where a security response to an incident can in turn create new risks leading to potential escalation.

Above all, project workers, contractors, consultants shall be oriented on the security precautionary measures required, entrance and exist, code of conducted to be followed whenever there are security risks.

In this regard, the security personnel have clear rule of engagement set out in the code of conduct for security personnel. Accordingly, they are required to treat all persons humanely and with respect for their dignity and privacy and will be accountable to any breach of Code of conduct for security personnel on the SMP. Regarding rules for the use of force, the security personnel are engaged in a manner consistent with applicable law and the minimum requirements contained in the section on Use of Force in this Code and agree those rules with the Client. The security personnel will only, guard, transport, or question detainees if: (a) the Company has been specifically contracted to do so by a state; and (b) its Personnel are trained in the applicable national and international law. Besides, they are required to treat all detained persons humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment. In addition, security personnel are required to treat all apprehended persons humanely and consistent with their status and protections under applicable human rights law, including in

particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Furthermore, security personnel are guided by the GBV Action Plan and are strictly prohibited to engage in or benefit from, sexual exploitation (including, for these purposes, prostitution) and abuse or gender-based violence or crimes, either within the Company or externally, including rape, sexual harassment, or any other form of sexual abuse or violence, forced labour, child labour, discrimination etc.

Generally, security personnel are responsible for protection of people, property and environment. For the project, the security personnel ensure protection of people (program workers, contractors and visitors) and asset/property (program, client, workers etc.) through executing roles and responsibilities including but not limited to:

- Assess the day to day security situation of the project site and its surrounding.
- Controlling access/Conduct body search at camp access points strictly implement check in and out procedure (Control the movement of people, vehicles (Ensure vehicle log is maintained), and materials coming into and out of their site).
- Conduct regular security patrol and safety hazard inspection to deter crime and safety related hazards in the site.
- Timely communicate/report imminent security threats, safety hazards and incident to contractor.
- Create awareness and implement Security Operating Procedure and Security Code of Conduct (e.g. Rules for the use of force).
- Establish and maintain good and healthy relationship with local community and project workers.
- Collaborate and work with local government security structure as per the rules of engagement.
- Play leadership role during security emergency situations before contractor, security focal person or police turn to guidance.
- Properly use surveillance system and turn lights timely.
- Manage crowd with extreme care in cases of site dispute occurrence.
- Treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers or children.
- Not engage in any form of sexual abuse and harassment including unwelcome sexual advances, requests for sexual favors, and other unwanted verbal or physical conduct of a sexual nature with other Contractor's or Employer's Personnel and members of the community.

# 7 SECURITY ARRANGEMENTS

# MANAGEMENT

The security management arrangements for the project lies in the government structure. Accordingly, the EAPP-PIU/EEP-PIU will strictly rely on and work with the key security players regional, district and village level as required based on the scope and magnitude of the security risks. This will help to have smooth communication of security alerts, incident reporting, and incident response in collaboration with relevant stakeholders, community relationships, etc. The chain of command and communication structure of the National Police Service will be used. All the security personnel be guided good practice principles such as proportional response, human right consideration, interconnection, community engagement, gender consideration.

## 7.1 Oversight and Control of Security Operations

EAPP-PIU and EEP-PIU Coordinators are responsible for the overall security risk management related to the project. Whereas security focal persons at regional, district and village level are responsible and accountable for supervision and control of security issues through working different relevant stakeholders, the daily supervision of performance of security force for the subproject shall be done by the contractor and security focal person at operational level.

Specifically, EAPP-PIU and EEP-PIU will be responsible for:

- a) As part of sub-project screening, undertake security risk assessment and recommend mitigation measures;
- b) Ensure that security mitigation measures are included in sub-project Environment Social Management Plan (ESMPs);
- c) Monitor potential security risks on sub-project sites together with the local government
- d) Provide training for concerned stakeholders to mitigate social risks of project workers and equipment including security risks;
- e) Ensure that project Grievance Redress Mechanism (GRM) established for the project and implemented and that project workers are informed about the GRM procedure;
- f) Report periodically to the World Bank on the implementation of the SMP.

In the case of security personnel are contracted by implementing agencies and contractors/sub- contractors and have control over the personnel contracted for the project, the PIU have responsibility of monitoring security issues. In this regard, contractors/sub- contractors shall abide by national law, ESS4, Environment and Social Framework Good Practice Note on Security Personnel and International Code of Conduct for Private Security Service Providers. In this regard, the contractor are to ensure that 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. So as ensure the safety and security of their employees. Although security is often sub- contracted, ultimately, the EAPP-PIU/EEP-PIU is responsible for the commitments made on the project.

## **7.2 Community Engagement**

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. 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. This should be implemented as per the SEP.

## **7.3 Security Management and Monitoring plan**

The security assessment, follow up and monitoring shall be conducted EAPP-PIU/EEP-PIU on a weekly basis. Findings of the follow up and monitoring will be filled, analyzed, interpreted and reported. Besides the EAPP-PIU/EEP-PIU will work with all key government security players at regional and federal level. In addition, information from the security institutions shall be proactively communicated to project workers, contractors, consultants etc.

**Table 7—1. Security Management Plan**

No.	Potential SecurityRisk	Prevention and mitigation measures	Responsible body	Implementation period	Indicative Budget (USD)
1	Theft of equipment and material	<p>Implementing access control system - secure and monitor entrance and outlet points of the workplace, proper badge and visitor card system, etc;</p> <ul style="list-style-type: none"> <li>■ Not leaving visitors unattended in the workplace.</li> <li>■ Ensuring proper security lighting;</li> <li>■ Where necessary, recruit and retain security guards who have experience;</li> <li>■ Conduct regular inventory of program assets;</li> <li>■ Minimize the amount of valuables and cash carried;</li> <li>■ Seek advice from local staff as to local areas considered unsafe;</li> <li>■ Train and aware project workers on security plan and context of the area.</li> </ul>	Regional, Zone, Woreda, Kebele and PIU Contractors and sub-contractors	Throughout the program implementation	50,000
2	Burglary and vandalism	<ul style="list-style-type: none"> <li>■ Maintenance and up-grading of access control and surveillance systems</li> <li>■ Install security lights to ensure visibility camps, facilities and material storage areas</li> <li>■ Ensure proper fencing that is responsive to different security contexts</li> <li>■ Have full time security personnel at the facilities andcamp site</li> <li>■ Establish formal and consistent reporting and communications mechanisms with public security forces and</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	100,000

		<p>government officials in the project area;</p> <ul style="list-style-type: none"> <li>Train and aware project workers on security plan and context of the area</li> </ul>			
3.	Conflicts within work environment	<ul style="list-style-type: none"> <li>Conduct regular training and security awareness programs for project workers;</li> <li>Ensure functionality of workers GRM;</li> <li>Adhere to Labor Management Procedure</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	50,000
4.	Community unrest	<ul style="list-style-type: none"> <li>Provide training and awareness creation on precautionary measures need to be taken during community unrest;</li> <li>Ensure program related operational GRM that communities including disadvantaged groups, minorities can use to raise their dissatisfaction and ensure that community program related concerns are addressed in a timely manner</li> <li>Undertake stakeholder engagement and community dialogues to get the views and concerns of communities as per SEP;</li> <li>Increased vigilance should be implemented during periods of community unrest;</li> <li>Any event having a potential to change the security situation within the operational areas must be communicated to management so that appropriate steps can be taken.</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	200,000
5.	GBV/SEA	<ul style="list-style-type: none"> <li>Induct security personnel on the project's CoC and ensure contracted security personnel sign the CoC</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	

		<ul style="list-style-type: none"> <li>■ Strengthen treatment and referral pathways for GBV/SEA survivors</li> <li>■ Raise awareness on GBV/SEA protocols for the Project in line with LMP</li> <li>■ Provide separate ablution facilities for men and women at the workplace</li> <li>■ Ensure proper lighting on the compounds</li> <li>■ Fully implement sanctions contained in the GBV Action Plan (Please refer GBV Action Plan)</li> </ul>			
6	Risks emanating from use of security personnel	<p>The Project will be guided by the National Laws while addressing security concerns. The World Bank's ESF provides for possible mitigation measures for security personnel engaged in Bank financed projects which include the following:</p> <ul style="list-style-type: none"> <li>■ Monitor risks resulting from acts of security personnel;</li> <li>■ Manning sub-project sites;</li> <li>■ Make reasonable inquiries to verify that the direct or contracted workers providing security are not implicated in past abuses;</li> <li>■ Raise awareness to contracted security personnel or determine that they are properly trained in the use of force and appropriate conduct towards workers and affected communities;</li> <li>■ Review allegations of unlawful or abusive acts of security personnel.</li> <li>■ Ensure security personnel contracted under the project are inducted on and sign the CoC.</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	200,000

		<ul style="list-style-type: none"> <li>■ Report incidents related to use of security personnel.</li> <li>■ MoU will be signed (where applicable).</li> </ul>			
7.	Insecurity during transit	<ul style="list-style-type: none"> <li>■ There is a risk of vehicles being ambushed while transporting staff, equipment and materials to sub project sites. This can be prevented/mitigated by: <ul style="list-style-type: none"> <li>■ Obtaining intelligence information regarding vulnerable routes and avoiding travels during risk periods</li> <li>■ All project workers and visitors must have the appropriate information and security clearance before undertaking any travel;</li> <li>■ Transport goods and workers during the day to reduce the risk of attack;</li> <li>■ Ensure travelers have backup food, water, communication apparatuses (e.g. mobile phone), etc.</li> <li>■ Report incidents</li> </ul> </li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation.	100,000
8.	Risk related to armed conflict and kidnapping	<ul style="list-style-type: none"> <li>■ Assign security focal person who will closely follow and closely communicate.</li> <li>■ Ensure good contacts with national law enforcement agencies, with a view to obtaining the best possible protection for project workers.</li> <li>■ Ensure up-to-date, detailed instructions project workers on security situations and precautions they should take in relation to the implementation of the security plan, including a comprehensive listing of emergency supplies they should have</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	100,00

		<p>on hand and guidance on their behavior during a variety of emergencies, including armed conflict;</p> <ul style="list-style-type: none"> <li>■ Project workers should familiarize themselves with information provided to them regarding the security management system at their location;</li> <li>■ Keeping the federal and regional Program Manger informed, on Safety and Security, of all developments in the subproject area which might have a bearing on the security and protection of the staff project workers for decision.</li> <li>■ Train and aware project workers on security management plan and security context of the subproject area.</li> </ul>			
		<p>Kidnapping:</p> <ul style="list-style-type: none"> <li>■ Use of physical security personnel,</li> <li>■ Ensure consistent reporting and communications mechanisms with public security forces and other stakeholders.</li> <li>■ Staff should avoid travel in darkness; only using trusted drivers / ; not set patterns and routines; keep in pairs or teams at all times.</li> <li>■ Local knowledge of the program/subproject area and operational context must be maintained by staff at all times.</li> <li>■ Seek information from project security focal person and clearance from PIU coordinator.</li> </ul>			

		<ul style="list-style-type: none"> <li>■ Any event having a potential to change the security situation within program areas must always be communicated to PIU Coordinator so that appropriate steps can be taken.</li> <li>■ SMP should be made available to all staff and appropriate training conducted.</li> <li>■ Never fight back when apprehended with armed people</li> <li>■ Do not try to argue or make provocative comments.</li> <li>■ Do not stare or make eye contact with the kidnappers.</li> </ul>			
9.	Environment and OHS Risk	<ul style="list-style-type: none"> <li>■ Conduct regular training and awareness program LMP, ESHS Guidelines, OHS, safety hazards, programs for project workers, community.</li> <li>■ Environmental and Social Clauses for Contractors Consultation</li> <li>■ Adhere to Hazardous material and Wastes Management set out in the ESMF</li> <li>■ Adhere to Labor Management Procedure.</li> <li>■ Adhere to Liquid and Solid Waste Management Plan</li> <li>■ Ensure ESHS/OHS provisions are incorporated in the bidding documents and contract agreement for construction.</li> <li>■ Ensure that waste management is operable to reduce the fuel element for fire</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	100,000

		<ul style="list-style-type: none"> <li>■ Ensure a fire alarm/smoke alarm system is operable within the Agricultural research centres</li> <li>■ Conduct regular Environmental and Social Monitoring and audit.</li> <li>■ Conduct regular emergency drills at project sites in coordination with relevant local authorities.</li> <li>■ Report incidents related to OHS.</li> </ul>			
10	Exposure to natural hazard (flooding)	<ul style="list-style-type: none"> <li>■ Aware workers on potential flood vulnerable areas and seasons.</li> <li>■ Get out of low areas subject to flooding during raining.</li> <li>■ Evacuate immediately to high ground, if you think you are at risk or are advised to do so</li> <li>■ Never try to walk or swim through flowing water.</li> <li>■ Be aware of flash flood areas such as canals streams, drainage channels.</li> <li>■ Wait until it is safe to return.</li> <li>■ Monitor Weather Radio, local television and radio stations before, during or after flooding.</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	100,000
11	Risk of traffic accident	<ul style="list-style-type: none"> <li>■ Properly implement Road Traffic Safety Assessment and Management Plan prepared for project.</li> <li>■ Vehicles should be serviced and well maintained.</li> <li>■ Staff should be briefed on what to look for when hiring a vehicle in a remote location.</li> <li>■ Training of drivers in advanced First Aid should be a priority.</li> <li>■ Hire or train drivers on changing of essential parts of vehicles if required.</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	50,000

		<ul style="list-style-type: none"> <li>■ Train drivers on Road Traffic Safety Assessment and Management Plan</li> </ul>			
12.	Medical risk	<ul style="list-style-type: none"> <li>■ Project workers should be trained on basic first aid services.</li> <li>■ First aid packs must be availed to the site and field visit.</li> <li>■ The team has ascertained availability of emergency services in case of medical emergency.</li> <li>■ Persons carrying medications have more than enough for the whole trip and appropriate storage means.</li> <li>■ The team has self-disclosed to fellow team members relevant medical conditions / history in event unable to recount details themselves.</li> <li>■ Records/letters with history/ medication in local language are being carried.</li> </ul>	PIU, Contractors and sub-contractors Security players in the government structures	Throughout the program implementation	100,00

## **8 Annex**

### **8.1 SECURITY OPERATING PROCEDURES**

#### **Common Operating Procedures**

##### **Physical Security**

The project contractors will be required to prepare and submit site and subproject specific SMPs at the region and specific sites where the subcomponents of the project will be implemented, varies. The SMP shall capture the specific site potential risks and assess the specific physical security, internal and external security risks and submit to the project coordination unit.

##### **Communications**

Communications with employees and contractors will be critical to ensuring a safe work environment. Certain selected employees' supervisors working on the site and contractors working on the project will be required to carry a two-way radio. This is because cell phone coverage may be limited. The two-way radio will be capable of providing emergency notification and alerting of any security incidence. The project team will work closely with the contractor and supervise consultants to develop a program to ensure proper communications during the construction, including identification of procedures and equipment for summoning emergency assistance from the local authorities.

##### **Construction Security**

To reduce risks, public access to the project site will be restricted. All project staff and visitors will access the project areas through designated gates. Searches will be conducted by security personnel who have received instruction and information regarding the procedure and legal aspects of searches and seizure.

##### **Fencing**

Fencing system will be implemented to restrict public access to the project site. Access point gates will be constructed and will be closed and secured. Contracted security guards will monitor the gates at all times and only allow authorized visitors and workers.

##### **Exterior Lights**

Exterior lighting will be strategically placed, when possible, to emphasize perimeters, gate access points and entry ways, as well as key areas.

##### **Security Guards**

The project will employ experienced security guards, preferably from the local community. Guards will be trained on security risks, occupational health and safety risks (OHS), and emergency response protocols. Guards will be assigned to maintain boundary security, control access points, screen individuals and vehicles, and ensure compliance with security protocols. Body searches will only be conducted by security personnel of the same gender as the party searched. Security patrols shall be carried out by the security personnel.

##### **Project Vehicles**

All project vehicles must be parked within secured compound. All vehicles must be licensed and checked periodically. They must have spare tires and first aid kit. Drivers must abide by all traffic rules and not exceed speed limits. They must also report immediately any traffic incident.

**Prohibited Items.**

Items such as guns, knives, alcohol, drugs and explosives will be prohibited from the project site. This prohibition applies to both workers and visitors.

**Reporting of Security Incidences**

Any security incidence related to the project shall be immediately reported to the project manager or security personnel in charge and shall be properly documented.

**Travel Security**

Travel security shall be required where project staff and equipment are transiting through areas with insecurity. Travel to high-risk areas should be kept at minimum and should be subject to a security risk assessment prior to the said travel.

**Security Approach**

To ensure security the project will work with all relevant stakeholders within and across institutions or organizations. In this regard, 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. Dialogue with communities about security issues can help to identify potential risks and local concerns and can serve as an early warning system. Besides, PMU and Contractors shall communicate their security arrangements to workers and communities, subject to overriding safety and security needs. In addition, community members should be aware of their ability to make complaints without fear of intimidation or retaliation. Because security personnel often are the first point of contact with community members at the project locations, they should also be informed about their role in community relations and about the grievance mechanism and key issues of concern to local communities. To help guide the community engagement for the project, stand-alone Stakeholder Engagement Plan has been prepared and disclosed.

Furthermore, grievance redress mechanism shall be established in the government devolving structure. Additionally, the World Bank grievance redressing services will also be available. The project-level grievance mechanism shall accept concerns or complaints regarding the conduct of security personnel and that such concerns and complaints, as well as any associated evidence and facts, be promptly documented and assessed and action be taken to prevent recurrence. The responses implemented in response to complaints are monitored and the outcomes communicated to relevant parties, taking into account the need to protect the confidentiality of victims and complainants. Besides, the establishment of functional and accessible Grievance Redress Mechanism (GRMs) would help to reduce the risk of community members resorting for protest and roadblock to draw attention to their grievance in situation where a security response to an incident can in turn create new risks leading to potential escalation.

Regular follow up and monitoring shall be conducted. Findings of the follow up and monitoring will be filled, analyzed, interpreted and reported. Additionally, the project team will work with all key government security players at regional and federal level. In addition, information from the security institutions shall be proactively communicated to project workers, contractors, consultants etc.

Above all, project workers, contractors, consultants shall be oriented on the security precautionary measures required, entrance and exist, code of conducted to be followed whenever there are security risks.

In this regard, the security personnel have clear rule of engagement set out in the code of conduct for security personnel. Accordingly, they are required to treat all persons humanely and with respect for their dignity and privacy and will be accountable to any breach of Code of conduct for security personnel on the SRAMP (refer Code of Conduct for security personnel annex 9). Regarding rules for the use of force, the security personnel are engaged in a manner consistent with applicable law and the minimum requirements contained in the section on Use of Force in this Code and agree those rules with the Client. The security personnel will only, guard, transport, or question detainees if:

1. The Company has been specifically contracted to do so by a state; and
2. Its Personnel are trained in the applicable national and international law. Besides, they are required to treat all detained persons humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment. In addition, security personnel are required to treat all apprehended persons humanely and consistent with their status and protections under applicable human rights law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Furthermore, security personnel are guided by the GBV Action Plan and are strictly prohibited to engage in or benefit from, sexual exploitation (including, for these purposes, prostitution) and abuse or gender-based violence or crimes, either within the Company or externally, including rape, sexual harassment, or any other form of sexual abuse or violence, forced labour, child labour, discrimination etc.

Generally, security personnel are responsible for protection of people, property and environment. For FSRP, the security personnel ensure protection of people (program workers, IAs, contractors and visitors) and asset/property (program, client, workers etc.) through executing roles and responsibilities including but not limited to:

- Assessing the day-to-day security situation of the project site and its surroundings.
- Controlling access and conducting body search at camp access points. Strictly implementing check in and out procedure (controlling the movement of people and vehicles) and materials coming into and out of the project site.
- Conducting regular security patrols and safety hazard inspection to deter crime and safety related hazards in the site.
- Timely communicate and report imminent security threats, safety hazards and incidents to contractors and site security focal persons.
- Create awareness and implement security operating procedure and security code of conduct, for example, implement rules to follow on the use of force.
- Establish and maintain good working relationship with local community and the project workers.
- Collaborate and work with the local government security force as per the rules of engagement.
- Play a leadership role during security emergency situations.
- Properly use surveillance system and turn lights timely.
- Manage crowd with extreme care in cases of site dispute occurrence.
- Treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers or children.

- Not engage in any form of sexual abuse and harassment including unwelcome sexual advances, requests for sexual favors, and other unwanted verbal or physical conduct of a sexual nature with other Contractor's or Employer's Personnel and members of the community.

## 8.2 Escalation Matrix

State Alert Level	Alert State Green	Alert State Yellow	Alert State Orange	Alert State Red	Alert State Black
Descriptor	Precautionary	Restriction of movement	Stabilization	Concentration	Relocation/Evacuation
Potential Triggers	<ul style="list-style-type: none"> <li>-Agreement by project coordination units at all level and with stakeholders;</li> <li>-Agreement between project implementers and project workers;</li> </ul>	<ul style="list-style-type: none"> <li>Community unrest/conflict;</li> <li>-Limitation of transportation access to project site</li> <li>-Limitation of access to target Sites due to insecurity;</li> <li>-Government offices affected in undertaking their day to day activities</li> </ul>	<ul style="list-style-type: none"> <li>-All yellow Status Triggers, and additionally:</li> <li>-Specific threats against workers;</li> <li>➤ Community unrest risk;</li> <li>➤ Temporary program delays;</li> <li>➤ Non-life-threatening injury to project personnel;</li> <li>➤ Loss or damage to assets;</li> </ul>	<ul style="list-style-type: none"> <li>All orange status Triggers, and additionally:</li> <li>Armed conflict in the project vicinity seriously impacting project activities;</li> <li>Only essential operational travel should be considered Management Unit;</li> <li>Severe costs to the program major disruption of activities</li> <li>Projects may be suspended at short notice;</li> <li>Serious injury and possible death to project personnel;</li> </ul>	<ul style="list-style-type: none"> <li>-All red Status triggers, and additionally:</li> <li>- Death or severe injury of team member;</li> <li>-Withdrawal of WB Supported projects from the area (or nearby) location;</li> <li>-Withdrawal/lack of government support to ensure security;</li> <li>-Critical unrest/conflict in neighboring impacting on project activities</li> <li>-Ongoing operations are unsustainable and projects may be suspended for indefinite periods</li> </ul>

<p>Project Response</p>	<p>Normal day to day government operations ongoing</p> <p>-Project activity ongoing</p> <p>-Project coordinators and security focal personnel monitor the security situation.</p>	<p>-undertake site specific security risk assessment</p> <p>- The public security officials to notify project coordinators who will in turn notify project workers within 24 hours.</p> <p>Government security officers accompany project workers, contractors and suppliers during movement to project site</p> <p>-Temporary suspension of activities;</p>	<p>-Project workers pause field visit to move to safe location;</p> <p>-Project coordinators and security focal personnel to account for workers and project resources regularly.</p> <p>- The public security officials to notify project coordinators who will in turn notify project workers immediately,</p> <p>- Public security officials in liaison with the PIU assess potential for de-escalation.</p> <p>- Update WBG on proposed options for de- escalation for agreement</p> <p>- Implement agreed de-escalation actions</p> <p>-Temporary suspension of activities;</p>	<p>-Project workers to move to concentration points and prepare to relocate to safe location;</p> <p>- Project coordinators and security focal personnel to account for workers and project resources regularly</p> <p>-The public security officials to notify project coordinators who will in turn notify project workers within 24 hours.</p> <p>-Update WBG on proposed options for de-escalation for agreement</p> <p>-Implement agreed de-escalation actions</p> <p>-Suspension of project activities</p>	<p>The public security officials to notify project coordinators who will in turn notify project workers within 24 hours</p> <p>Project to review viability of continuing with project activities in a particular location/region</p> <p>Project to advise and agree with WBG on proposed way forward (pause/continue/otherwise)</p> <p>Suspension of project activities.</p>
-------------------------	---	--	--	--	--