**FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA**

 ****

**MINISTRY OF INNOVATION AND TECHNOLOGY**

**EASTERN AFRICA- REGIONAL DIGITAL INTEGRATION PROJECT SOP II (P180931)**

**FINAL**

**SECURITY RISKS ASSESSMENT AND MANAGEMENT PLAN (SRAMP)**

 **OCTOBER 2023**

 **ADDIS ABABA, ETHIOPIA**

Table of Contents

[LISTS OF ACRONYMS iv](#_Toc146519869)

[1. Introduction 1](#_Toc146519870)

[1.1. Project Background 2](#_Toc146519871)

[1.2. Project Overview 3](#_Toc146519872)

[1.3. Objective of the Security Risk Assessments and Management Plan 5](#_Toc146519873)

[2. Methodology for Security Risk Assessment and Management Plan 6](#_Toc146519874)

[2.1. Key Informant Interview: 6](#_Toc146519875)

[2.2. Video Conference and Virtual Consultation 6](#_Toc146519876)

[2.3. Consultation conducted by Afar Regional State Science, Innovation and Technology Commission 7](#_Toc146519877)

[2.4. Community consultation 8](#_Toc146519878)

[2.5. Consultation with Disadvantaged or vulnerable groups 8](#_Toc146519879)

[2.6. Sampling Procedure 9](#_Toc146519880)

[2.7. COVID-19 precautions 9](#_Toc146519881)

[3. Review of National Policies and Legal Frameworks 10](#_Toc146519882)

[3.1. National Polices and Legal Frameworks 10](#_Toc146519883)

[3.1.1. 10](#_Toc146519884)

[3.2. Ethiopian Relevant Laws and Regulations 11](#_Toc146519885)

[3.3. The World Bank Environmental and Social Framework Requirement 13](#_Toc146519886)

[4. Security Risk Assessment 15](#_Toc146519887)

[4.1. Objective of the Security Risk Assessment 16](#_Toc146519888)

[4.2. Scope of the Security Risk Assessment 16](#_Toc146519889)

[4.3. Security Context and Threat Assessment 16](#_Toc146519890)

[4.3.1. Security Context in Ethiopia and IGAD Member States 16](#_Toc146519891)

[4.4. Security Risk Assessment Identification 20](#_Toc146519892)

[4.5. Project Areas Potential Security Risks and Mitigation Measures 20](#_Toc146519893)

[4.5.1. Potential Security Risks Identification 20](#_Toc146519894)

[4.6. Security Risk Analysis and Evaluation 25](#_Toc146519895)

[4.7. Security Risk Rating and Prioritization 27](#_Toc146519896)

[4.8. Security Analysis and Evaluation Results 27](#_Toc146519897)

[4.8.1. Key Security Threats 29](#_Toc146519898)

[4.8.2. Key Security Threats-Specific to Sample Project Areas 32](#_Toc146519899)

[4.8.3. Key Security Threats-Risk matrix Summary 38](#_Toc146519900)

[4.8. Mitigation Measures 41](#_Toc146519901)

[5. Security Management Plan 53](#_Toc146519902)

[5.1. Purpose of the Security Management Plan 53](#_Toc146519903)

[5.2. Objectives of the SMP 53](#_Toc146519904)

[5.3. Scope of the SMP 54](#_Toc146519905)

[5.4. Security Management Plan Governance 54](#_Toc146519906)

[5.5. Overview of Security Management Plan 55](#_Toc146519907)

[5.6. Security Management Procedures for EA-RDIP 56](#_Toc146519908)

[5.7. Oversight and Security Management 57](#_Toc146519909)

[5.8. Communication Protocols 58](#_Toc146519910)

[5.9. Grievance Redress Mechanism 59](#_Toc146519911)

[5.9.1. Key Steps in Security-Related GRM Process 59](#_Toc146519912)

[5.9.2. Procedures to manage risks of sexual harassment from security personnel 61](#_Toc146519913)

[5.9.3 Measures to Manage OHS Risks to Security Personnel 62](#_Toc146519914)

[5.10. Operational Security 63](#_Toc146519915)

[5.11. Performance Monitoring and Reporting 69](#_Toc146519916)

[5.11.1. Site Visits 69](#_Toc146519917)

[5.11.2 Oversight 70](#_Toc146519918)

[5.11.3 Joint Implementation Supervision Mission (JISM) 70](#_Toc146519919)

[5.11.4. Independent Security Audit 71](#_Toc146519920)

[5.11.5. Communicating the Outcome of Complaints 71](#_Toc146519921)

[5.12 Managing Public or Government Security Engagement 72](#_Toc146519922)

[5.12.1. Signing a Memorandum of Understanding 72](#_Toc146519923)

[5.12.2. Communication and engagement with public security 73](#_Toc146519924)

[5.13. The Estimated cost of risk mitigation and prevention measures for the project 74](#_Toc146519925)

[Annex 1: Escalation Matrix 86](#_Toc146519926)

[Annex 2- Security Operating Procedures (SOP) 88](#_Toc146519927)

[Annex 3: EA-RDIP II related incident and accident reporting procedure 92](#_Toc146519928)

[Annex 4: Security incident registration form for sub projects of EA-RDIP II 93](#_Toc146519929)

[Annex 5: Occupational Health and Safety incident registration form for sub projects of EA-RDIP II 94](#_Toc146519930)

[Annex 6: Steps to conduct Root Cause Analyses (RCA) for a Workplace Accident 95](#_Toc146519931)

[Annex 7: Content of a Safeguards/Standards Corrective Action Plan (SCAP) Outline 96](#_Toc146519932)

[Annex 8: Code of Conduct for Contractors’ 100](#_Toc146519933)

[Annex 9: Code of conduct of security personnel 103](#_Toc146519934)

[Annex 10: List of SRAMP Study Participants 106](#_Toc146519935)

**LIST OF TABLES**

[Table 1: Summary of EA-RDIP components and related activities 4](#_Toc120946265)

[Table 2: Participant Organizations and Individuals in Key Informant Interview, Video Conference and Virtual Consultation. 7](#_Toc120946266)

[Table 3: Summary of articles from the FDRE constitution related to human right, protection and security 10](#_Toc120946267)

[Table 4: Summary of Ethiopian relevant laws and regulations 12](#_Toc120946268)

[Table 5: Summary of World Bank environmental and social framework requirements 13](#_Toc120946269)

[Table 6: Probability of Security Risk Occurrence 25](#_Toc120946270)

[Table 7: Risk Security Description and Rating 25](#_Toc120946271)

[Table 8: Risk Matrix 26](#_Toc120946272)

[Table 9: Risk level and priority indicators 27](#_Toc120946273)

[Table 10: Summary of key security threats identified 29](#_Toc120946274)

[Table 11: Calculated security risk value of Afar Regional State for EA-RDIP 34](#_Toc120946275)

[Table 12: Calculated security risk value of Gambella regional state for EA-RDIP 35](#_Toc120946276)

[Table 13: Numbered list of security threats in sample regional states of EA-RDIP 38](#_Toc120946277)

[Table 14: Afar Regional State-Risk Matrix 39](#_Toc120946278)

[Table 15: Gambella Regional State-Risk Matrix 39](#_Toc120946279)

[Table 16: Somali Regional State-Risk Matrix 40](#_Toc120946280)

[Table 17: Summary of potential security threats and mitigation measures 42](#_Toc120946281)

[Table 18: Summary of risks and management framework for SRA and SMP 75](#_Toc120946282)

# LISTS OF ACRONYMS

ABHR Alcohol Based Hand Rub

AfCFTA African Continental Free Trade Area

AIDS Acquired Immunodeficiency Syndrome

BoE Bureau of Education

BoEPA Bureau of Environmental Protection Authority

BoH Bureau of Health

BoLS Bureau of Labor and Skill

BoLUA Bureau of Land Use and Administration

BoPD Bureau of Pastoral Development

BoTI Bureau of Trade and Industry

BoWSA Bureau of Women and Social Affairs

CapEx Capital expenditures

CAPP Cluster Area Project Personnel

CLS Cable Land Station

COVID-19 Coronavirus Disease

CSIRT Computer Security Incident Response Team

DBE Development Bank of Ethiopia

DE4A Digital Economy for Africa

EAC East African Community

EACO East African Communication Organization

EA-RDIP II Eastern Africa Regional Digital Integration Phase II

ECA Ethiopian Communications Authority

EDFP Ethiopian Digital Foundation Project

EIC Ethiopian Investment Commission

EPA Environmental Protection Authority

E&S Environmental and Social

ESF Environmental and Social Framework

E&S Environmental and Social

ESCP Environmental and Social Commitment Plan

ESMP Environmental and Social Management Plan

ESS Environmental and Social Standards

EthERNet Ethiopian Education and Research Network

FCV Fragility, Conflict, and Violence

FM Financial Management

FCSC Federal Civil Service Commission

FY Fiscal Year

G2P Government-to-People

GBV Gender-based Violence

GoE Government of Ethiopia

GRC Grievance Redress Committee

GRM Grievance Redress Mechanism

GRS Grievance Redress Service

HoA Horn of Africa

HIV Human Immunodeficiency Virus

HTC HIV Testing and Counseling

ICT Information Communications Technology

ID Identification

IDA International Development Association

IDP Internally Displaced People

IFC International Finance Corporation

IGAD Intergovernmental Authority on Development

ILO International Labor Organization

IP Internet Protocol

IPC Infection Prevention and Control

ISP Internet Service Providers

IT Information Technology

IXP Internet Exchange Point

km Kilometer

LMP Labor Management Procedures

MDAs Ministries, Departments and Agencies

M&E Monitoring and Evaluation

MFD Maximizing Finance for Development

MICT&PS Ministry of Information and Communication Technologies and Postal Services

MInT Ministry of Innovation and Technology

MNO Mobile Network Operators

MOCT Ministry of Communications and Technology (Federal Republic of Somalia)

MoE Ministry of Education

MoF Ministry of Finance

MoH Ministry of Health

MoLS Ministry of Labor and Skill

MoTRI Ministry of Trade and Regional Integration

M&S Monitoring and Supervision

MoU Memorandum of Understanding

NIDPO National ID Program Office

NLUA National Land Use and Administration

NREN National Research and Education Network

NPSCs National Project Steering Committees

NTCs National Technical Committees

OHS Occupational Health and Safety

OPGW Optical Ground wire

P2B People-to-Business

P2P People-to-People

PAFP Project Area Focal Person

PDO Project Development Objective

PIM Project Implementation Manual

PIU Project Implementation Unit

PKI Public Key Infrastructure

PPE Personal Protective Equipment

PPP Public-Private Partnership

PSC Project Steering Committee

PSNP Productive Safety Net Project

RAN Radio Access Network

REC Regional Economic Communities

REN Research and Education Networks

RPIU Regional Project Implementation Unit

RPSC Regional Project Steering Committee

RPTC Regional Project Technical Committee

SARS-COv-2 Severe Acute Respiratory Syndrome Coronavirus-2

SDM Single Digital Market

SEA Sexual Exploitation and Abuse

SEP Stakeholder Engagement Plan

SH Sexual Harassment

SOP Series of Projects

SMP Security Management Plan

SRA Security Risk Assessment

SRAMP Security Risk Assessment and Management Plan

STD Sexually Transmitted Diseases

TA Technical Assistance

TVET Technical and Vocational Education and Training

UN United Nation

UNHCR United Nations Higher Commission for Refugees

USF Universal Service Fund

WHO World Health Organization

WPTF Woreda Project Task Force

ZTE Zhong Xing Telecommunication Equipment

# Introduction

Security assessment and management begins with the mandate and commitment of the management and governance bodies of the institution, and is followed by design of a framework, implementing risk management, monitoring and review of framework, and lastly, continuously improving the framework. Establishing an effective risk framework is an essential aspect of good corporate governance for all companies and should be a key priority for boards of directors and senior management. The implementation of a security risk assessment and management framework requires the appropriate risk department for the size of and complexity of the organization. In Fragile and Conflict Vulnerable (FCV) area almost all implementing institutions are required to have a head of security risk assessment and management, with officers or departments responsible for different areas of risk. For Ethiopia, the area that is generally least developed is operational risk, and this requires the greatest attention.

The teams involved in managing the SRA and MP operations have the greatest awareness of what is required and what can go wrong and should be included as early as possible in the planning process of a World Bank financed project’s SRA and MP. This provides a very useful counterbalance to the digital sector development teams who often fail to anticipate the risks in the strategies that they are promoting or see risk assessment as an impediment to progress. Hence, this report intends to identify the risks related to the potential internal and external security threats and their impacts on the Project implementation process, Project implementing parties including the communities, government staff, the project implementation teams including Project Implementation Unit (PIU)/ Ministry of Innovation and Technology (MoInT), partners organizations Ethiopian Communication Authority (ECA), Ethiopian Education and Research Network (EthERNeT), Ministry of Trade and Regional Integration (MoTRI) and the World Bank team while undertaking their customary assignments and develop strategic plan to mitigate the envisaged impacts.

The security risk assessment and management plan considers i) scanning on the possibility an unfortunate occurrence of potential security threats, ii) assess the potential of the PIU, community, and the World Bank team to contain unwanted, negative consequences of an event, iii) develop a mechanism to avoid or mitigate the consequences of the East African-Regional Digital Integration Project/EA-RDIP SOP II activity and associated uncertainties, iv) incorporating all tools and methods required to handle the severity of a security threats in a way that promotes human value, v) identifying and addressing capacity building needs to overcome the deviation from a reference value and associated uncertainties resulted from security threats; and vi) develop budgets to apply to risk assessment, response and management activities.

1.1. Project Background

Phase II of the Series of Project (SOP-II) will include two countries from the HoA region, within Eastern Africa – Ethiopia, Djibouti and extend support three Regional Economic Communities/RECs[[1]](#footnote-1) (East African Communities/EAC[[2]](#footnote-2) East African Communication Organizations/EACO and Intergovernmental Authority on Development/IGAD). Country projects under Phase II will first and foremost focus on inclusive digital transformation through regional digital market development, with a focus on extending universal access to broadband internet and digitally enabled services.. As noted above, selected countries under SOP-II have some of the largest gaps in the region in relation to connectivity and Djibouti have a high undersea cable connectivity potential. Meanwhile, EACO, EAC and IGAD were selected based on their mandate and membership, which allows for full geographic coverage of the whole Eastern Africa region, including the Horn of Africa/HoA sub-region. Their increasingly overlapping membership also allow for potential synergies across sub-regions that can facilitate the integration process. In subsequent phases, it is envisioned that more countries or RECs will be able to join the SOP basis their readiness and commitment to the SOP’s goals. SOP-II will focus on expanding the program to select countries in the HoA (i.e. Djibouti, Ethiopia) with the aim of building on investments under SOP-I through complimentary interventions in neighboring countries, towards the goal of developing a single digital market in the region.

The Social Risk is Substantial at concept[[3]](#footnote-3). The implementation of the components 1, 2 and 3 of EA-RDIP has the potential for impacts on community health and safety including transmission of diseases, including sexually transmitted infections and potentially communicable disease (depending on the evolving nature of the disease ). Risks associated with the use of any security personnel during construction are assessed. We have considered both the private and government personnel to secure work sites. Given the potentially remote and geographically distributed nature of activities as well as any security considerations supervision of these requirements will be a bit challenging. The Project proposes activities to harmonize policies for and legal framework for data privacy, protection and security.

These Technical Assistance (TA) activities would need to be undertaken in line with the World Bank guidance. Establishing foundational ID systems, provision of public and private services online and data exchange all bring about risks associated with data security. Poor E-waste handling and disposal could expose people to non-dioxin-like polychlorinated biphenyls, polycyclic aromatic hydrocarbons, polychlorinated dibenzo-p-dioxins, polychlorinated dibenzofurans and dioxin-like polychlorinated biphenyls. Most of these compounds are endocrine groups and indigenous peoples must be considered in the project to ensure their inclusion, that collected data cannot be used as a basis for discrimination (e.g. on the basis of religion, ethnicity, sexual orientation and gender identity etc.) and that data protection covers such groups as needed.

The SRA and MP is complemented by the Social Assessment which has focused to assess the social risks and proposes a progressive and well-tailored Social Development Plan. It is also further supported by Labor Management Procedures which deals with risks related to project workers, and risks to the community as a result of expansion of digital infrastructure will require a construction workforce and may result in labor influx. This has the potential for impacts on community health and safety including transmission of diseases, including sexually transmitted infections and potentially communicable disease (depending on the evolving nature of the disease). As a result, in additions to other Environment and Social Risk Management tools; the preparation of the Security Risk Assessment and Management Plan will help to provide potential strategic options to address the identified security risks and mitigate the impacts.

## 1.2. Project Overview

**Project Objective:** The EA-RDIP Project Development Objective (PDO) is to advance regional digital market integration through increasing access to broadband connectivity and strengthening the enabling environment for digital service delivery. In Ethiopia, specifically, the Project will support connectivity, data and online market development and integration.

 **Components of the project:** The project is designed around five integrated and mutually reinforcing components, which reflect the distinct but interconnected layers of an integrated regional digital market. Components 1, 2 and 3 will support Connectivity Market Development and Integration; Data Market Development and Integration; and Online Market Development and Integration, respectively, whereas component 4 will support Project Management and Implementation Support (at regional and national level). In additions to the above project components, component 5 is dedicated for Contingency Emergency Response Component and will allow for rapid reallocation of uncommitted national IDA funds in the event of an eligible emergency declared in one of the participating countries. These components include a menu of activities from which Borrowers (Ethiopia and Djibouti), have selected activities to be implemented under Series of Project/SOP-II, based on their most pressing needs. In addition, components include activities to be undertaken by RECs (EAC and IGAD) to help coordinate and advise countries in the region, ensuring that all benefit from the larger contiguous regional market supported by the project. The Project would have the following four components (see on table 1 below):

Table 1: Summary of EA-RDIP components and related activities

|  |  |
| --- | --- |
| **COMPONENT** | **Activities** |
| **Component 1: Connectivity Market Development and Integration** |
|  1.1: Cross border and backbone network connectivity | 1,500 KM of new fiber five additional routes to the sea and rehabilitation of terrestrial cablesPrivate capital mobilization[[4]](#footnote-4) |
|  1.2: Last mile connectivity including in borderland areas | To connect remote, rural, borderland locations where the commercial incentive for last-mile network expansion is insufficient (host communities and Internally Displaced Person (IDP)/refugees camps in borderland areas). Tigray region is included as a beneficiary under conflict affected regions category. |
|  1.3: Enabling legal, regulatory and institutional ICT environment | Activities financed will support reforms that aim to catalyze further investments in climate-smart digital infrastructure and attainment of universal access targets |
| **Component 2: Data Market Development and Integration** |
|  2.1: Cyber-security frameworks, infrastructure and capacity | To strengthen and harmonize cyber-security frameworks, build capacity for responding to cyber threats/cybercrimes and create greater awareness on cyber-security. |
|  2.2: Data exchange, governance and protection | To improve the efficiency of data storage, transmission and build resilience for government data storage. |
| **Component 3: Online Market Development and Integration** |
|  3.1: Digital enablers for cross-border trade and service delivery | Support to build readiness for partaking in regional trade initiatives will be provided. Project financing will cover capacity building to Ministry of Innovation and Technology (MInT) and the Ministry of Trade and Regional Integration (MoTRI) for facilitating participation in regional trade agreements and expanding cross-border e-services. |
|  3.2: Regional research and education networks (RENs) and training for digital skills  | To strengthen the higher educational network through expansion and integration of Ethiopia Education and Research Network (EthERNet) with regional Research and Education Networks (RENs) allowing for network economies in unit prices for capacity purchase and knowledge transfer. |
| **Component 4: Project Management and Implementation Support** | This component would finance the Project Implementation Unit -PIU’s (at MInT) operations for project implementation. Implementation would entail functions of project management and coordination, including procurement, financial management (FM), and M&E, as well as environmental and social safeguards management. |
| **Component 5: Contingency Emergency Response Component** | CERC will help strengthen the institutional capacity to respond to emergencies caused by climate and natural disasters, and support reinforcing the country’s resilience to climate and natural risks identified above. |

##  1.3. Objective of the Security Risk Assessments and Management Plan

**General Objective**

The overall objective is to conduct overall security risk assessment of the EA-RDIP II and develop an integrated security management plan to improve the level of safety and security for communities, project workers, implementing agencies and World Bank team involved in the project.

**Specific objectives**

* To understand the existing status and level of security risk assessment being practiced in the implementation of WB financed digital sector project in Ethiopia ;
* To identify and evaluate the relevance of the existing security risk assessment standards and frameworks being applied nationally and internationally to the WB financed digital sector project in Ethiopia;
* To identify gaps in the existing security management practices in the WB financed digital sector project in Ethiopia; and
* To propose mitigation measures and security management plan relevant for the identified security risks and impacts related to the EA-RDIP II.

# Methodology for Security Risk Assessment and Management Plan

**Study design:** The SRA and SMP study is cross-sectional pre-test/posttest design with no control group.

## 2.1. Key Informant Interview:

Key informant interview (KII) has been conducted with relevant stakeholders from federal to woreda level. Table 2 presents the summary of the participant organizations and people. The purpose of the KII with stakeholders is twofold. First, as part of an on-going project information disclosure, provide project information to allow stakeholders understand: (i) the purpose, nature, and scale of the project; (ii) the duration of proposed project activities; (iii) potential benefits, risks and adverse impacts of the project; (iv) the proposed stakeholder engagement process highlighting the ways in which stakeholders can participate in designing, implementing and monitoring SRA and MP; and (v) the process and means by which grievances can be raised and will be addressed. The second purpose is intended to assess the views and concerns of the stakeholders and incorporate inputs in the preparation of the SRA and MP for EA-RDIP. Accordingly, the key informant interview with relevant federal level stakeholders has been conducted from October 10 to November 4, 2022; stakeholders in Afar region from November 09-13, 2022; and stakeholders Elidar woreda in Halli-Lofefele connectivity route in Afar region from November 18-21, 2022. Annex 10 gives detail contract address of the participant organizations and key informant interview.

## 2.2. Video Conference and Virtual Consultation

Unlike for Afar region, the Bank security clearance was not obtained for the face-to-face interview with the stakeholders in Somali and Gambella regions. The security risks in Somali region are posed due to the recent war with the Al-Shebab terrorist group and the current political instability in the region. The source of security risks in Gambella region is associated with the recurring attacks from the Murule armed clan from South Sudan. To mitigate these security risks, consultation with stakeholders in Somali and Gambella region has been conducted through video conference and virtual consultation. The consultation with stakeholders in Somali region was conducted through video conference on October 28, 2022, whereas consultation with stakeholders from Gambella region was done on November 16, 2022 through virtual consultation using Microsoft Teams. Both the video conference and virtual consultation was facilitated by the MInT team. The summary of the participant organizations and people in video conference and virtual consultation is given in Table 2.

## 2.3. Consultation conducted by Afar Regional State Science, Innovation and Technology Commission

Due to the World Bank security protocol, we (consultants) were not allowed to go to Elidar Woreda located in Afar regional state. As a result, we worked in collaboration with MInT with Digital Transformation Program Office and MInT-Directorate to Councils and Regions Coordination; we have provided orientation on Woreda level stakeholder and community consultation to experts working in Afar regional state’s Science, Innovation and Technology Commission. Apparently, the experts have conducted the Woreda level stakeholder consultation starting from November 15, up to November 23, 2022. The summary of the stakeholder consultation participants is also included on table 2, below.

Table : Participant Organizations and Individuals in Key Informant Interview, Video Conference and Virtual Consultation.

|  |  |  |
| --- | --- | --- |
| ***Name of organization*** | ***Number of KII*** | ***Level of Stakeholder Group*** |
| Ministry of Innovation and Technology | 3 | **Federal** |
| Ethiopian Communication Agency  | 1 |
| Ministry of Trade and Regional Integration | 1 |
| National Research and Education Networks | 1 |
| Development Bank of Ethiopia | 4 |
| Ethiopian Investment Commission | 1 |
| Ethiopian Environmental Protection Authority | 2 |
| Ministry of Women and Social Affairs | 1 |
| National ID Program Office  | 2 |
| Afar Region Trade and Industry Bureau | 2 | **Regional** |
| Afar Region Science, Innovation and Technology Commission  | 5 |
| Afar Region Women and Children Affairs Bureau | 1 |
| Afar Region Peach and Security Bureau | 1 |
| Afar Region Rural Land Use and Administration Bureau | 1 |
| Afar Region Environmental Protection Bureau | 1 |
| Somali Region Innovation and Technology Bureau\* | 5 |
| Somali Region Women and Children Affairs Bureau\* | 2 |
| Somali Region Environmental Protection Bureau\* | 3 |
| Gambella Region Innovation and Technology Commission\*\* | 2 |
| Gambella Region Peace and Security Bureau\*\* | 1 |
| Gambella Region Women and Children Affairs Bureau\*\* | 1 |
| Elidar Woreda Trade Office\*\*\* | 1 | **Woreda** |
| Elidar Woreda Rural Land Use and Administration Office\*\*\* | 1 |
| Elidar Woreda Environmental Protection Office\*\*\* | 1 |
| Elidar Woreda Women and Children Affairs Office\*\*\* | 1 |
| Elidar Woreda Peace and Security Office\*\*\* | 1 |

* *Indicates regional stakeholder consultation sessions conducted through virtual-video conference.*

*\*\* Indicates regional stakeholder consultation sessions conducted through virtual-Microsoft Teams.*

 *\*\*\* Indicates Woreda stakeholder consultation sessions conducted through experts from Afar-Science, Innovation and Technology Commission.*

## 2.4. Community consultation

To have a representative sample, it was planned to undertake one community consultation in each of the three connectivity route. As planned, the community consultation in Haweli Kebele along the Halli-Ellidar-Lofefelo connectivity route in Afar region has been conducted. It was held at the Galafi village on November 18, 2022 in which 18 participants took part. With the aim to capture the views and concerns of all segments in the local community including disadvantaged or vulnerable groups, the participants were composed of clan leader, religious leaders, community representative, women, youth, person with disability and refugee. The minutes, sample photos and attendance sheet of this community consultation are annexed herewith (see ***Annex 10***). However, the consultant has not been provided with the Bank security clearance to conduct the community consultation in the Bameza-Abugedaf connectivity route in Dima Woreda Gambella Region and Dollo-Oddo connectivity route in Dollo Woreda Somali Region. Also, the consultant made unsuccessful efforts to conduct community consultation through virtual meeting due to lack of internet connection and other means of communication in these two areas. With no other option, the client (MInT) was responsible to undertake the community consultation in the two connectivity routes either by deploying its own staff or in cooperation with its line Bureau in the respective regions. Yet, the client organization was unable to do so justifying lack of finance for per diem and logistic for transportation to the areas as a problem.

## 2.5. Consultation with Disadvantaged or vulnerable groups

To capture the views and concerns of disadvantaged or vulnerable groups, the participants of community consultation composed of women, youth, person with disability and refugee. Special emphasis was paid to these disadvantaged or vulnerable groups by taking into account their views and special concerns to be incorporated in the preparation of this SRA and MP.

## 2.6. Sampling Procedure

The preparation of this SRA and MP employed sampling procedures that allow to achieve representativeness both in terms of geographic and stakeholder coverage. To obtain geographic representativeness, the sample selection and assessment for this SRA and MP covered all the project areas: (a) the Halli-Ellidar-Lofefelo to depicts the E&S situation along the Ethio-Djbouti cross-border connectivity route; (b) Bameza-Abugedaf to capture the trans-boundary connectivity between Ethiopia and South Sudan; and (c) Dollo-Oddo to reveal the situation of the Ethio-Somalia cross border connectivity.

The sampling technique has given a similar attention for the inclusiveness of the appropriate stakeholders by apply the following procedures. First, as highlighted in sub-sections 2.1., 2.2., and 2.3., the selection for stakeholder consultation covered key stakeholders (the main implementing agency, partner organizations, main direct beneficiaries, and public private partnership) from federal to woreda level. Second, the engagement of the local community has been captured through community consultation. Finally, the sampling procedure applied ways to represent the views and concerns of the vulnerable and disadvantaged groups: disadvantage or vulnerable groups were proportionately included during the selection of the participants for community consultation; and organizations for disadvantaged or vulnerable groups such as Ministry of Women and Social Affairs and the line regional bureau and woreda office were consulted for the special concerns of these groups and incorporated in the preparation of this SRA and MP.

## 2.7. COVID-19 precautions

Currently, there is no COVID-19 pandemic lockdown in Ethiopia or in the project target areas. Despite this, the stakeholder consultation process was carried out observing COVID-19 protocols (such as wearing face masks, keeping physical distance, using hand sanitizer), as per the national and WB prevention protocol on the pandemic.

# 3. Review of National Policies and Legal Frameworks

## 3.1. National Polices and Legal Frameworks

The Federal Democratic Republic of Ethiopia (FDRE) has formulated several development policies, proclamations and strategies to improve the livelihood and to promote sustainable development of Ethiopian people in general and the rural communities in particular. The policies, strategies and legal frameworks that are reviewed and discussed in the following sections are directly or indirectly applicable during the implementation of EA-RDIP II.

3.1.1. The Constitution of Ethiopia

 The Constitution of the FDRE is the highest policy and legal document that lays the basis for all laws and policies in the country. The Constitution of FDRE provides a number of basic and comprehensive principles that consider social protection and management in the country including the sustainable development. It recognizes the existence of diverse socio-cultural groups, including historically disadvantaged and underserved communities, pastoralists, agro-pastoralists and minorities as well as their rights to socioeconomic equity and justice. The relevant articles to security risks and impacts provisions among others are identified below:

Table : Summary of articles from the FDRE constitution related to human right, protection and security

|  |  |  |
| --- | --- | --- |
| **No** | **Article** | **Description** |
| 1 | Article 14: Rights to life, the Security of Person and Liberty  | This article states that every person has the inviolable and inalienable right to life, the security of person and liberty. |
| 2 | Article 15: Right to Life | 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. |
| 3 | Article 16: The Right of the Security of Person | Everyone has the right to protection against bodily harm. |
| 4 | Article 17: Right to Liberty | 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.No person may be subjected to arbitrary arrest, and no person may be detained without a charge or conviction against him. |
| 5 | Article 18: Prohibition against Inhuman Treatment | Sub article 1 in this article states that everyone has the right to protection against cruel, inhuman or degrading treatment or punishment. |
| 6 | Article 25: Right to Equality | 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. |
| 7 | Article 24. Right to Honor and Reputation | Everyone has the right to respect for his human dignity, reputation and honor,Everyone has the right to the free development of his personality in a manner compatible with the rights of other citizens,Everyone has the right to recognition everywhere as a person. |
| 8 | Article 26: Right to Privacy | Article 26(1) state that everyone has the right to privacy. This right shall include the right not to be subjected to searches of his home, person or property, or the seizure of any property under/his personal possession. |
| 9 | Article 28: Crimes against Humanity  | Article 28(1) states that criminal liability of persons who commit crimes against humanity, so defined by international agreements ratified by Ethiopia and by other laws of Ethiopia, such as genocide, summary executions, forcible disappearances or torture shall not be barred by statute of limitation. Such offences may not be commuted by amnesty or pardon of the legislature or any other state organ. |
| 10 | Article 32: Freedom of Movement | Article 32(1) states that any Ethiopian or foreign national lawfully in Ethiopia has, within the national territory, the right to liberty of movement and freedom to choose his residence, as well as the freedom to leave the country at any time he wishes to. |
| 11 | Article 37: Rights of Access to Justice | Everyone has the right to bring a justifiable matter to, and to obtain a decision or judgment by, a court of law or any other competent body with judicial power. |
| 12 | Article 42: Rights of Labor | Article 42(2) stipulates that ‘workers have the right to a healthy and safe work environment’, obliging an employer (be it government or private) to take all necessary measures to ensure that workplace is safe, healthy and free of any danger to the wellbeing of workers. |
| 13 | Article 44: Environmental Rights | Article 44(1) stipulates all persons have the right to live in clean and healthy environment. |
| 14 | Article 87: Principles for National Defense | Article 87(3) it states that the armed forces shall protect the sovereignty of the country and carry out any responsibilities as may be assigned to them under any state of emergency declared in accordance with the Constitution. |
| 15 | Article 90: Social Objectives | Article 90(1) states that to the extent the country’s resources permit, policies shall aim to provide all Ethiopians access to public health and education, clean water, housing, food and social security. |
| 16 | Article 92: Environmental Objectives | Government shall endeavor to ensure that all Ethiopians live in a clean and healthy environment. |

## 3.2. Ethiopian Relevant Laws and Regulations

The environmental and social impacts of development should be assessed in order to ensure that projects, as much as possible, must be environmentally sustainable and socially acceptable. In one way or another, this ultimately contributes to ensure sustainable development. In this regard, policies, legislative frameworks, guidelines and standards have been developed by the government of Ethiopia to contribute for the enhancement of sustainable development. The relevant policy, legal and administrative frameworks of the government of Ethiopian and the policies of the World Bank have been reviewed in the following sections.

Table : Summary of Ethiopian relevant laws and regulations

|  |  |  |
| --- | --- | --- |
| **No** | **National laws and regulations** | **Description** |
| 1 | National Social Protection Strategy of Ethiopia -2012 | The general objective to create an enabling environment in which citizens (including people with special need and other vulnerable groups have the right to equitable access to all social protection services that will enhance their growth and development. Ethiopia’s social protection policy is a central public policy component for addressing poverty, vulnerability and inequality. |
| 2 | Proclamation No.1097/2018Definition of Powers and Duties of the ExecutiveOrgans of the Federal Democratic Republic ofEthiopia | In relation to Gender Based Violence, proclamation No. 1097/2018, article 28 bestows powers and duties to the Ministry of Women, Children and Youth to: “design strategies to effectively prevent and take measures against gender-based violence against women; implement same in collaboration with relevant organs; facilitate the setting up centers for provision of holistic health, psychological, legal and rehabilitation services for women who were victims of violence; and follow up the implementation of same.” Moreover, program specific GBV Action Plan has been prepared for EA-RDIP (Please refer GBV Action Plan Annex 6 on the ESMF). |
| 3 | Ethiopian National Policy on Women-1993 | States 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.” |
| 4 | National Policy on Empowerment of Women-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 incidence. Institutions and mechanisms/schemes 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." |
| 5 | 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.” |
| 6 | Labor Proclamation No. 1156/2019 | The proclamation under its Part Seven, Chapter One, and Article 92 of this proclamation deals with occupational safety, health and working environment, prevention measures and obligations of the employers. Accordingly, the Proclamation obliges the employer to take the necessary measure for adequate safeguarding of the workers in terms of their health and safety.In addition, in this proclamation under its Part Six, Chapter1 and 2 described about women and young safety that women are not assigned on the works that may risk to women health and also overnight work including night shift work.Regarding young employees, organizations do not hire young personnel less than 15 years old and if they hire young between age 15 and 18 years, they should not allow to work more than 7 hours per day and also overnight work including night shift work.Moreover, the Occupation Health and Safety Directive provides the limits for occupational exposure to working conditions that have adverse impacts on health and safety.Women shall not be discriminated against as regards employment and payment on the basis of their sex.It is prohibited to employ women on type of work that may be listed to be particularly odious or harmful to their health; an employer shall not terminate the contract of employment of women during her pregnancy and until four months of her confinement reformulated by Labour Proclamation No.156/2019 as until four months after her confinement. Grant leave to pregnant women without deducting her wage; adhere to the occupational health and safety requirements provided in the proclamation; take appropriate steps to ensure that workers are properly instructed and notified concerning the hazard of their respective occupation and the precautions necessary to avoid accident and injury to health; provide workers with protective equipment, clothing and other materials and instruct them of its use; and Ensure that the work place and premises do not cause danger to the health and safety of the workers.Furthermore, the Proclamation defines the occupational safety and health, and working environment focusing on (i) preventive measures, (ii) occupational injuries, (iii) defining degree of disablement, (iv) benefits to employment injuries, (v) medical services. The provisions associated to OHS are delineated on part seven of the Labor Proclamation 1156/2019, from Article 92-112. |

## 3.3. The World Bank Environmental and Social Framework Requirement

Three Environment and Social Standards (ESS) among the 10 ESS comprising the World Bank Environmental and Social Framework (ESF) are relevant for this Security Risks Assessment. ESS1: Assessment and Management of Environmental and Social Risks and Impacts, ESS2 labor and working conditions and ESS4 community health and safety. Those environmental and social standards 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. The Security Risk Assessment (SRA) is a living document to facilitate project planning, preparation, and implementation. It is anticipated that the SRA will be updated as additional information becomes available during project implementation, including in relation to security of personnel/project workers, timing of project activities, and associated due diligence and social risk management.

Table : Summary of World Bank environmental and social framework requirements

|  |  |  |
| --- | --- | --- |
| **No** | **ESS and other standards** | **Description** |
| 1 | ESS1: Assessment and Management of Environmental and Social Risks and Impacts | The main objective of this Standard is to identify, evaluate and manage the environment and social risks and impacts of the project in a manner consistent with the ESSs. As the result adopt mitigation hierarchy approach to:- Anticipate and avoid risks and impacts;- Where avoidance is not possible, minimize or reduce risks and impacts to acceptable levels;- Once risks and impacts have been minimized or reduced, mitigate; and- Where significant residual impacts remain, compensate for or offset them, where technically and financially feasible. |
| 2 | ESS2: Labor and Working Conditions | The main objectives of WB ESS 2 are the following: - To promote safety and health at workplace.- To promote the fair treatment, non-discrimination, and equal opportunity of project workers.- To protect project workers, including vulnerable workers such as women, persons with disabilities, children (of working age, in accordance with this ESS) and migrant workers, contracted workers, community workers, and primary supply workers, as appropriate.- To prevent the use of all forms of forced labor and child labor.- To support the principles of freedom of association and collective bargaining of project workers in a manner consistent with national law.- To provide project workers with accessible means to raise workplace concerns. |
| 3 | ESS4: Community Health and Safety | The main objectives of WB ESS 4 are the following: - To anticipate and avoid adverse impacts on the health and safety of project-affected communities during the project life cycle from both routine and non-routine circumstances.-To promote quality and safety, and considerations relating to climate change, in the design and construction of infrastructure, including dams.- To avoid or minimize community exposure to project-related traffic and road safety risks, diseases and hazardous materials.- To have in place effective measures to address emergency events.- To ensure that the safeguarding of personnel and property is carried out in a manner that avoids or minimizes risks to the project-affected communities. |
| 4 | The World Bank Group (WBG) Environment, Health and Safety (EHS) Guidelines | The 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.  |
| 5 | Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel, | 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 EA-RDIP is also based on the Good Practice Note. Hence, the government of Ethiopia and implementing entities at all levels shall be abide by the World Bank Environmental and Social Framework, Environmental and Social Standards, Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel, ISO 31000 & other pertinent standards and rules. |

#

# 4. Security Risk Assessment

Security risk assessments set our insight into the dangers that EA-RDIP II project and, crucially, the staff face in project areas. A security risk assessment is a fundamental element of the risk management process is viewed as an integral part of the wider Environmental and Social Risk Management (ESRM) assessments involved in establishing operations or project in FCV country (like Ethiopia), whether implemented directly or by partners. The private entities involved on the project design or implementation are considered. The private sectors engage in to contract by accepting risks and seeking rewards, but they will discharge most or all responsibility conventionally procured separately and coordinated by the government. Hence, they can use SRA MP instruments and resources available within the PIU.[[5]](#footnote-5)A PIU’s relationship with private security should be managed through a formal process. The contract shall include requirements for security tasks and expectations of conduct as well as provisions for the client to review relevant documents and materials and to audit the security provider periodically and to terminate a provider’s services if the standards are not met. Furthermore, each private entity is contractually obliged to either operate under the project SRAMP or produce its own SRAMP, which is bridged to the project SRAMP, with the project SRAMP being the minimum acceptable standard.

This risk assessment process first identified the different security threats within EA-RDIP II context, and how your staff, assets, the sub-projects being implemented, or the organisation could be vulnerable. It then analysed according to likelihood and impact to determine the degree of risk involved. Finally, it identified and assessed the different options that could be undertaken to manage these risks. Furthermore, mitigating measures are identified, but it is likely there will still be some residual risk, which should be checked against your World Bank risk threshold to see if it is acceptable for the EA-RDIP II to continue. Following the risk assessment process and measures identifications, it is followed by rigorous management plan, because if it is not implemented MInT might be exposed as breaching its duty of care. This security risk assessment process is well documented and included key findings and proposed measures to manage the different risks. Risk assessments will be updated on a regular basis. In addition, staff will be provided with guidance on what the different likelihood and impact ratings mean in order to analyse more accurately the various threats and to ensure consistency throughout the EA-RDIP II implementation.

## 4.1. Objective of the Security Risk Assessment

The following are the main objectives of security risk assessment for EA-RDIP II:

* Identify, evaluate, and prioritize risks and likely security contexts and overall situations;
* Understand the main risks to staff, project beneficiaries and project-affected communities; assets and sub-projects (risk assessment system);
* Identify the potential threats faced along the course of implementation of EA-RDIP II; and
* Determine tools to evaluate threats and rating of risks.

## 4.2. Scope of the Security Risk Assessment

The consultant has used appropriate methodologies for the assignment including among others, situation analysis, risk analysis, vulnerability scan, review of key reference documents, interviews with key stakeholders, informants and technical staff, general observations, and focus group discussions. The assessment is undertaken in three Regional States and one woreda selected from each regional state particularly selected as representing to the three connectivity routes. This is intended to address key security challenges in those EA-RDIP II intervention Woredas with particular emphasis to challenges attributable to implementing EA-RDIP II activities at the regional and local levels.

## 4.3. Security Context and Threat Assessment

#### 4.3.1. Security Context in Ethiopia and IGAD Member States

#### 4.3.1.1. Security Context in IGAD Member States

IGAD notes that its member states are ‘listed among the thirty-five most fragile countries in the World’.[[6]](#footnote-6) Countries in the Horn of Africa are facing issues with regard to a complex mix of limited or uneven access to natural resources, social tensions among groups in society (regional, religious and ethnic), and poverty and economic inequalities. The weakness of state institutions to provide physical security, including the basic good of the survival of citizens, in combination with corruption, has resulted in ineffective governance, undemocratic practices, limited confidence, distrust in state authority and legitimacy, and insurgencies.[[7]](#footnote-7)

Conflicts in the region: Aside from intrastate disputes and insurgencies (affecting all countries in the region, in particular Somalia), the Horn of Africa has a long history of interstate disputes, cross-border violence and border conflicts. Some are fairly recent, such as Kenya’s and Somalia’s maritime border dispute (2014) over which country may rightfully control the resource-rich section of the Indian Ocean. This issue has been brought to the International Court of Justice. Both countries have support from different international actors (e.g. France and the USA support Kenya, and Norway and the United Kingdom support Somalia—all for reasons of relationships and access to claims), which complicates the situation.[[8]](#footnote-8) Yet, it is interesting to note that such disputes notwithstanding, cooperation and neighbourliness are still considered key by both governments for guiding the relationship between Kenya and Somalia.[[9]](#footnote-9)

Another border dispute is that between South Sudan and Sudan over territories rich in resources (oil and gas). The relationship between South Sudan and Sudan has been tense since South Sudan’s independence in 2011. In addition to internal power struggles in South Sudan, the main challenge has been to find a solution for border issues. Uganda is a key player in this regard, as it has supported South Sudan throughout the conflict. However, the focus is shifting from security to economic issues. South Sudan is also still facing an internal dispute over the establishment of a unity government, which is part of the peace deal from 2018. However, it has proven difficult to get to an agreement. The risk of instability, with subsequent effects on the region, therefore, remains.[[10]](#footnote-10)

Additionally, disputes over resource allocation and access have also been significant in the region. For example, the struggle for eastern Nile waters—involving mainly Egypt, Ethiopia and Sudan—has a long history. The negotiation of fair and equitable terms for water distribution has become more difficult with Ethiopia’s building of the Grand Ethiopian Renaissance Dam (GERD). The risk of escalation has led to offers for mediation by outside actors such as the USA.[[11]](#footnote-11)

These challenges notwithstanding, there are also opportunities for regional cooperation to tackle the megatrends mentioned above. Horn of Africa states are active in 11 multilateral organization: the African Union (AU), the Common Market for Eastern and Southern Africa, the Community of Sahel–Saharan States, the East African Community, the Gulf Cooperation Council, IGAD, the Indian Ocean Rim Association, the International Conference on the Great Lakes Region, the League of Arab States, the Nile Basin Initiative (NBI) and the Organization of the Islamic Conference. Together, they can create a range of forums and potential entry points for regional cooperation.[[12]](#footnote-12)

#### 4.3.1.2. Security Context in Ethiopia

Ethiopia has seen inter-communal violence and various ethnic insurgencies for over five decades.[[13]](#footnote-13) A number of inter-regional conflicts (e.g. Afar-Somali, Amhara-Oromia, Somali-Oromia, Tigray-Afar, Tigray-Amhara) make up a complicated conflict landscape across the country.[[14]](#footnote-14) Ethiopia’s current security situation is dominated by the on-going armed conflict between the federal government and the Tigray People’s Liberation Front (TPLF) that erupted in November 2020. The conflict in Tigray has contributed to extremely high levels of hunger and displacement, as well as significant loss of life.[[15]](#footnote-15)

Heightened levels of communal conflict over access to land and water following shifting politics at the federal level after the 2018 election, have led to the displacement of hundreds of thousands of people, especially in Oromia, the Southern Nations and the outskirts of Addis Ababa.[[16]](#footnote-16) In Tigray and Amhara, the UN finds that large numbers of the newly displaced have contributed to exacerbating existing tensions between Amharas and Tigrayans who previously lived together in the same areas. Tensions have exacerbated as internally displaced persons (IDPs) have not been provided with adequate food, nutrition, water, healthcare or sanitation.[[17]](#footnote-17)

There are dozens of armed actors operating across Ethiopia, and conflict over territory and cattle raiding are prevalent among different ethnic groups. Inter-pastoralist and pastoralist versus agro-pastoralist violence have ensued primarily over resources and cattle rustling/raiding.[[18]](#footnote-18) While a cattle raiding is a long-standing cultural practice among pastoralist groups, research suggests that it has become a more predatory activity, and several studies have found that resource conflicts have increased in severity as a result of the militarization of pastoralist societies.[[19]](#footnote-19) A cattle raiding is increasingly linked to livestock trading on foreign markets and small arms proliferation, which in turn increase incentives to engage in the activity. Evidence shows that young pastoralist men are hired and armed by wealthy individuals, including livestock traders, to carry out raids and at the same time reports of raids causing loss of human lives are increasing.[[20]](#footnote-20)

Very dry conditions have been found to increase both armed groups’ activity and violence between pastoralists and other livelihood groups, particularly when rains are absent during summer/*Kiremt*.[[21]](#footnote-21) This risk is higher in areas with existing ethno-political exclusion, where political and physical vulnerabilities can be mutually reinforcing and increase the likelihood that coping strategies take a violent form.[[22]](#footnote-22) Several studies find abundant rainfall to be associated with increased conflict risk as vegetation and resources impact armed groups’ tactical considerations concerning the timing and location of attacks.[[23]](#footnote-23) For instance, increased vegetation provides cover for raiders as high grass and dense bush cover make it easier to track and ambush cattle without being caught.[[24]](#footnote-24) In order to help prevent the consequences of climate change further exacerbating existing vulnerabilities and tensions, the AU, IGAD and UN system should support efforts to identify, analyze and respond to climate-related peace and security risks.

## 4.4. Security Risk Assessment Identification

The Security risks threats on the EA-RDIP areas are grouped as follows:

i. Internal security risk- caused by illegal, unethical or inappropriate behavior of the project staffs, temporary, part-time or seasonal employees or those directly affiliated with it.

ii. External security risks- These may include common criminal activity; disruption of the project asset for economic, political, or social purpose; and other deliberate (like sabotage the project activities) and non-deliberate actions (such as collateral damage caused by proximity to warring factions) that have a negative impact on the effective, efficient, and safe operation of the proposed project.

## 4.5. Project Areas Potential Security Risks and Mitigation Measures

### 4.5.1. Potential Security Risks Identification

 In rural area communities, livelihood systems can serve as a source of social instability. The encounter with rising cost of living, policy gaps, poor access to provision of services, lack of job opportunities and scarce resources has progressively exposed the vulnerability of the rural dwelling communities and it is eventually leading to social instability. The presence of undefined borders between Amhara and Tigray; Amhara and Afar, Amhara and Benishangul Gumuz; Amhara and Oromia; Oromia and SNNP; SNNP and Sidama; Benishangul Gumuz and Gambella; Afar and Somali; and among other bordering regional states is contributing to the outbreak of conflicts. This is endangering the safety and protection of individuals and natural resources in these areas. On the other hand, the presence of scarce resources and opportunities can be another driving factor. Apart from this; availability of poor basic services, high rate of unstable and unemployed youths supported by information and misinformation will pose a real danger and threat to the social cohesion of the individuals and groups in the project intervention areas.

 At macro-level; the interaction among the socio-economic and political factors, climate change will play a significant negative role on solving rural poverty and implementing local economic empowerment focused interventions or programs, and subsequent multidimensional security in Ethiopia. On the other hand, security risks are also categorized in to internal and external social risks. Among the vulnerable groups the following will be majorly affected: 1) the rural poor, 2) informal workers, 3) hard to reach communities like; women, girls, elderly, children, person with disabilities, PLWHIV, victims of COVID-19 and mentally ill people; 4) refuges and internally displaced persons; 5) petty trade workers and 6) prison populations.

At site level, there are occupational health and safety (OHS) risks to security personnel including:

(i) Risks related to traffic safety while traveling outside of the site and within the site.

(ii) Risks from unsafe ingress and egress to the site

(iii) Falling into open excavations while working near them

(iv) Risk of fall from heights such as watch towers

(v) Exposure to noise, vibration, and dust emission from the work area

(vi) Risks from working close of electricity/energy sources

(vii) Fall, slip, and trip risks due to poor housekeeping on the site

(viii) Biological hazards such as COVID-19, Sexually Transmitted Diseases/STDs, and pathogens from wastewater and solid waste in the work area

(ix) Physical hazards from prolonged exposure to weather (heat, cold, rainfall, etc)

(x) Psychological stress, burnout and health effect due to the demanding nature of the work including working irregular hours

(xi) Risks associated to preparedness and response in emergency situations resulting in bodily injuries and fatalities from crimes, violence, firearm accidents, etc.

(xii) Risks from exposure of all OHS hazards identified for project works (please see the Labor Management Procedures for detailed OHS risks).

(xiii) Supervision of OHS on regular and frequent bases in line with the requirements of the LMP (see the LMP for details onOHS risks).

(xiv)\_Using the hierarchy of control creates a systematic approach to managing OHS in the workplace by providing a structure to select the most effective control measures to eliminate or reduce the risk of certain hazards that have been identified as being caused by the operations of the EADRIP II implementation. The hierarchy of control has five levels of control measures, the most effective measure is at the top of the hierarchy and the least effective is at the bottom. So the idea is that, start from the top of the hierarchy in choosing the appropriate control measure. Where elimination is not feasible, measures should be taken to reduce the risk by following the hierarchy in the recommended order. Do not simply jump to the easiest control measure to implement. Risk control can be applied at the source of the hazard, through engineering controls, administrative controls and personal protective equipment (PPE). The detailed discussion on 5 stages of OHS control measures is presented below.



Figure : Five leve;s of OHS control measures

* + 1. ***Elimination-Physically remove the hazard(s):***

Elimination, or physically removing a hazard from a workplace, is the most effective stage of the hierarchy of controls. When hazards are eliminated or removed from a work environment, they no longer have the potential to negatively impact employees.

Though it’s conceptualized as the most effective stage, elimination is also typically the most challenging to implement. Doing so can be costly and require major overhauls in preexisting workplace processes.

Examples:

* Redesign a process to eliminate the use of hazardous equipment or product
* Perform tasks at ground level rather than working high above ground
* Store goods at lower heights so workers don’t have to climb tall heights and risk fall injuries or fatalities
	+ 1. ***Substitution-replace the hazard(s):***

Substitution, or replacing a hazardous item or activity with something less hazardous, is the second-most effective stage of safety control. Substitution serves a similar purpose to elimination, as it removes a hazard from the workplace or decreases the potential for the hazard to negatively affect employees. If a workplace process is still in its design or development phase, substitution can be an inexpensive and streamlined method for managing a hazard.

Examples:

-Replace a caustic cleaning agent with a non-toxic alternative

-Substitute a solvent-based paint with water-based paint

-Use a non-silica abrasive material instead of sandblasting

* + 1. ***Enginering controls-isolate people from the hazard(s):***

Engineering controls, or designing purposeful solutions that physically separate employees from hazards, are the third-most effective stage of safety control. Many organizations favor engineering controls to remove the hazard at the source, rather than after an employee comes into contact with a hazard. It’s important to note that while engineering controls can sometimes be costly to implement, they typically result in lower overall operating costs due to the new safety features.

Examples:

-Place barriers around fans and other loud machinery

-Fence around dangerous high-voltage equipment

-Install guardrails at worksites that are high above ground

* + 1. ***Administrative controls-change the way people work:***

Administrative controls, or changes to the way employees work and perform particular processes, are the fourth-most effective stage of safety control. Administrative controls are typically employed alongside other existing processes in which hazards are not totally controlled.

Organizations sometimes favor administrative controls due to their low-cost nature, but such initiatives are often somewhat ineffective and require significant effort on the part of affected employees.

Examples:

-Limit the time a worker is exposed to a hazard

-Create written formalized operating procedures

-Install signs, labels and alarms

* + 1. **Personal protective equipment (PPE)-protect workers:**

PPE, physical equipment worn or used by employees while they perform their work, are the fifth- or least-most effective stage of the hierarchy of controls.

Like administrative controls, PPE is typically used alongside preexisting processes that haven't completely controlled the occupational hazard. Using PPE as a safety control is typically very costly in the long term and can be somewhat ineffective if worn or used improperly.

Examples:

-Eye and face protection (goggles and masks)

-Head protection (hard hats)

-Foot and leg protection (foundry shoes)

-Hand and arm protection (chemical-resistant gloves)

-Body protection (hazmat suits)

-Hearing protection (earplugs)

(xv) It is also vital to develop procedures for development of OHS risk assessment and safe work system.

A) The employer, in consultation with workers and their representatives, should set out in writing an OHS risk assessment and safe work system procedure, which should be:

✓ specific to the organization and appropriate to its size and the nature of its activities;

✓ concise, clearly written, dated and made effective by the signature or endorsement ofthe employer or the most senior accountable person in the organization;

✓ communicated and readily accessible to all persons at their place of work;

✓ reviewed for continuing suitability; and

✓ made available to relevant external interested parties, as appropriate.

B) The OHS proceure should include, as a minimum, the following key principles and objectives to which the organization is committed:

✓ protecting the safety and health of all members of the organization by preventing work related injuries, ill health, diseases and incidents;

✓ complying with relevant national laws and regulations, voluntary programmes, collective agreements on OHS and other requirements to which the organization subscribes;

✓ ensuring that workers and their representatives are consulted and encouraged toparticipate actively in all elements of the OHS management system;

✓ continually improving the performance of the OHS management system; and

✓ The OHS management system should be compatible with or integrated in othermanagement systems in the organization.

## 4.6. Security Risk Analysis and Evaluation

For security risk analysis and evaluation, the approach involves two factors that are stated as follows. First, is the probability with which is the measure of certainty that an event, or risk, will occur. This can be measured in a number of ways, but for the EA-RDIP assigned a probability as defined in the Table 6 below:

Table 6: Probability of Security Risk Occurrence

|  |
| --- |
| Probability of Occurrences |
| Likelihood (L) | Meaning | Rating  | Likelihood per year |
|  Very likely | Occurs frequently-Will be continuously experienced unless action is taken to change events | 5 | 21-25 |
| Likely | -Occur less frequently if process is corrected- Issues identified with minimal activity | 4 | 15-20 |
|  Moderately likely | - Occurs sporadically- Potential issues discovered during focused review. | 3 | 5-14 |
|  Unlikely | - Unlikely to occur- Minimal issue identification during focused review | 2 | 2-4 |
| Very unlikely | * Highly unlikely to occur
 | 1 | 1 |

Another unit of measurement in this regard is risk severity descriptions and ratings. The table that illustrates risk severity, potential triggering factors and rating number is presented below.

Table 7: Risk Security Description and Rating

| **Severity (S)** |  **Potential Impact** | **Rating**  |
| --- | --- | --- |
| Critical | * Death or severe injury, loss of vital equipment, critical costs/ multiple fatalities, significant delays to project delivery affecting overall project objective, etc.
* Verifying the Severity of OHS incidents which may lead to severe injuries or possible death (verifying whether fatal or non-fatal, type of injury and part of body injury).
 | **5** |
| Severe | * Severe injury or possible death, loss of important equipment, severe costs to the project major disruption of activities
* - Verifying the Severity of OHS incidents which may lead to severe injuries or possible death (verifying whether fatal or non-fatal, type of injury and part of body injury).
 | **4** |
| Moderate | *
* Injury, loss of equipment, moderate costs to the project delays in activities
 | **3** |
| Minor | * Possible injury, lossof possible equipment, minor costs and limited delays of activities
 | **2** |
| Negligible | - No or minor injuries, no or minor loss of equipments, negligible costs, minor disruption of activities | **1** |

Potential triggers for different alert states are indicated in Annex 1.

The security risk can be calculated using the following formula risk matrix as indicated in table 8.

 **Relative Risk = L\*S**  whereas, ‘‘L’’ stands for likelihood of occurrence and ‘‘S’’ stands for severity of impact

 By multiplying the likelihood score with the Impact score a Risk Score is generated for each threat scenario. These scores are plotted onto a risk matrix (see below):

 Table 8: Risk Matrix

|  |  |
| --- | --- |
| **Risk Matrix** | **Impact =Severity x Frequency** |
| **Severity** |
| **Negligible-1** | **Minor-2** | **Moderate-3** | **Severe-4** | **Critical-5** |
| **Likelihood /Probability of Threat** | **Very Likely****(75%+)/5** | **Medium -5** | **Medium-10** | **Medium-15** | **High-20** | **Unacceptable -25** |
| **Probable/likely****(55-74%)/4** | **Low-4** | **Moderate-8** | **Medium-12** | **High-16** | **Very High-20** |
| **Moderately Likely****(40-54%)/3** | **Low-3** | **Moderate-6** | **Medium-9** | **Medium-15** | **Medium-15** |
| **Unlikely****(25-39%)/2** | **Low-2** | **Low** | **Medium-6** | **Medium-8** | **Medium-10** |
| **Very Unlikely****(-24%)/1** | **Negligible (1)** | **Low** | **Low** | **Low** | **Medium-5** |

*Note:*

Negligible

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Unacceptable* |  | *Very High* |  | *High* |  | *Medium* |  | *Low* |  |  |

## 4.7. Security Risk Rating and Prioritization

Critical, high, medium, low, and negligible security risk ratings are assigned to activities based on their likelihood of risk occurrence and the severity of the risk. The severity column that best describes the risk result can be found using the risk matrix and relative risk value. Then, in the likelihood row, choose the best description for the possibility of the incident occurring. The risk level is indicated in the box at the intersection of the row and column. The relative risk value can be used to prioritize necessary activities for effectively managing the security risks associated with the proposed project. As a result, table 9 determines priority using the following ranges.

Table : Risk level and priority indicators

|  |  |  |
| --- | --- | --- |
| **Risk value**  | **Risk level**  | **Action** |
| **25** | **Unacceptable** | Ongoing activities ceases immediately and resumes after all threats are sorted |
|  **21-24** | **Very High** | Ongoing operations are unsustainable and projects may be suspended for indefinite periods. Implementation of relocation or evacuation plan, as applicable |
| **16-20** | **High** | It requires priority and immediate action to control the risk or to avoid minimize or treat through appropriate mitigation measures. |
| **5-15** | **Medium** | It requires a planned approach to control the risks and apply temporary measures if required.  |
| **2-4** | **Low** | It may be considered as acceptable and further reduction may not necessary. However if the risk can be resolved quickly and efficiently, control measures should implemented. |
|  **1** | **Negligible** | No need of further action |

## 4.8. Security Analysis and Evaluation Results

The ongoing conflict (Northern Part of Ethiopia) has also led to an increase in sanctions and restrictions on aid financing and funding, which may affect the liberalization process in the telecommunications market. For instance, the U.S. International Development Finance Corporation delayed its USD 500 million loan to finance Safaricom Ethiopia’s market entry. The United States also imposed a new sanctions regime on several Ethiopian parties, resulting from the conflict, and U.S. President Biden announced plans in November 2021 to remove Ethiopia from the African Growth and Opportunity Act, an important trade program.[[25]](#footnote-25)

At the time of this writing, the conflict in Ethiopia appears to have de-escalated and officially the peace treaty is signed. However, Ethiopia still faces ongoing military operations and numerous challenges as a result of the conflict, including a humanitarian crisis in the northern part of the country.[[26]](#footnote-26)

 Safaricom Ethiopia’s plans for significant investment in the country over the next five years may be influenced by the government’s ability to stabilize the territory and provide confidence for such long-term investments. The situation is fluid, with Safaricom’s chief executive officer confirming in early November 2021 that the company maintains its plans to invest and conduct operations in Ethiopia, despite evacuating its staff from the country around that same time.[[27]](#footnote-27) Safaricom has indicated that while it aims to carry out its plans as projected, it will adapt and reassess as the situation evolves.[[28]](#footnote-28)

The ensuing instability in Ethiopia pose a major threat to investment and development in the country. Further, the spillover effects from the conflict threaten regional stability, creating the potential for significant disruption to investment and development in the broader HoA and East Africa regions. An inability to address these concerns promptly will likely push Ethiopia, and the region, beyond the risk tolerance of potential investors and may present new obstacles in the form of increased sanctions and restrictions on aid and/or funding.[[29]](#footnote-29)

Through closing the broadband gap, component 1 will help support commitment on ‘jobs and economic transformation’ through increased use of connectivity. Component 2 and 3 activities that strengthen cyber security, data protection efforts, governance-technology solutions, and digital skills development will support commitment to strengthening ‘governance and institutions’ and Component 4 will aid in a ‘gender development’ through collection and use of gender disaggregated data in ICT.[[30]](#footnote-30)

The mix of different ethnic groups from across Ethiopia, and from neighboring countries, coupled with the lack of infrastructure ensures that tensions can quickly build, and inter-communal conflicts have become more common. There has been a marked increase in crime, especially from youth groups and non-government military factions, as well as acts of GBV. With different communities and populations living in close proximity, conflict over cattle, pastures and natural resources are common threat in Ethiopia. Tensions can be exacerbated by armed anti-government groups, capitalizing on people’s differences and ethnic identities and the ease of access to small arms in the country further contributes to these risks, which can pose serious risks in regard to the project.

The Social Risk Rating of this project is assessed as substantial. This is primarily linked to the acquisition of land for the deployment of digital infrastructure (which may lead to physical or economic displacement of inhabitants) and the potential tensions between incoming workers and local communities. The project will also contend with Fragility, Conflict and Violence (FCV) country contextual risks such as political instability (induced by potential civil unrest) and contextual GBV/SEA risks.

### 4.8.1. Key Security Threats

As per the assessment conducted and the review of relevant literatures, the following 17 security threats are identified both at regional (Afar, Gambella and Somali regional states) and Woreda (Elidar, Dima and Dolo Ado Woredas) levels. The summary of the major security threats identified are presented on the table below.

Table : Summary of key security threats identified

|  |  |  |
| --- | --- | --- |
| **Threat No.** | **THREAT TYPE** | **DEFINITION** |
| 1 | Armed Robbery/Raid | Armed Robbery / Raid Armed robbery of a project work site with intent to steal possessions and cash, scenario assumes possible fatalities and severe injuries. |
| 2 | Armed conflict between government and non-government forces | Threats arising in the context of armed conflict, for example at the hands of, or as a result of, the activities of armed forces and groups who are parties to a conflict. |
| 3 | Theft of construction materials | Stealing and using project materials for meeting personal interests during the construction and operation of project sub-activities |
| 4 | Access blockage to some regions, cities or woredas | In some project areas due to civil unrest or some groups state of dissatisfaction public or private access road or routes may unlawfully controlled, interrupted or blocked and prevent vehicular or individual access to the boundary of real property proposed for EA-RDIP. |
| 4 | Risk of GBV/SEA/SH | Labor influx can lead to an increased risk of sexual exploitation and abuse (SEA) notably of women and girls especially associated with construction activities and locations where camps are established. Sexual exploitation and abuse (SEA) especially due to extreme poverty situation which may see even young girls engaging in survival sex; transaction sex, sexual harassment (SH) and other forms of GBV. Sexual violence and GBV in the countries proposed under Phase 1 including Ethiopia are very high. In particular, sexual violence against women has been used as a tool of war with many forms of SEA including child marriage, FGM/C, rape and intimate domestic violence being normalized especially in conflict areas. Exploitative transactional sex, including for basic survival is seen as accepted practice although official data is lacking. Gender Based Violence used to terrorize local population or for personal gratification – may occur as part of a larger assault instigated due to project activity or be specifically targeted against specific project workers.Sexual exploitation: any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. Sexual abuse: the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions |
| 6 | Local conflict between ethnic groups and clans | Clan conflicts and personal revenge can engulf an area of operation, turning it into an active area of fighting resulting in casualties on all sides including project workers operating in the area who have nothing to do with the grievances of either side. Scenario assumes possible fatalities of project staff. |
| 7 | Labor influx and human trafficking | Labor influx can lead to an increased risk of sexual exploitation and abuse (SEA) notably of women and girls especially associated with construction activities and locations where camps are established.Human trafficking-project staffs, temporary workers and community workers may involve in the act of the use of force, fraud, or coercion and may be the combination of all three practices to obtain some type of labor or commercial sex act. |
| 8 | Trespassing | Community members or persons may enter to enclosed area/fenced area without permission and try to take advantage of the sub-project, asset or service facility. It may ultimately manifest in terms of vandalism, robbery or terrorism. |
| 9 | Community protests | Events and organized protests may take place in different project areas as a means of expression of community members dissatisfaction towards a given institution, political leader or administration. Threats may arise as a result of communal or intra-group tension, within the project beneficiaries. These may be along ethnic and/or religious lines or between the refugees/IDPs and the host population. These may arise from competition for scarce resources such as land, water or firewood. They can be directed against the humanitarian community in circumstances where the camp population perceives they have been offered insufficient information prior to a distribution or have developed unrealistically high expectations of assistance. |
| 10 | Unmet community expectation or where benefits sharing is perceiving to be lacking or unfair | Community members may express their frustration to the miss-match among the community expectation and the actual outcomes of the project activities. They may assume that some community members, woredas, cities or even regional states are benefiting more compared to their condition or status. |
| 11 | Acts of violence | Threats arising from a general break-down in law and order may include, individual and/or collective criminal acts. This may include the threat of physical, mental, sexual or other harm or suffering, which may result in injury, death, physical or mental disability or deprivation. These are generally understood as acts of violence organized by groups against civilians or other non-combatant targets.  |
| 12 | Burglary of work place/residence | Individuals or groups may unlawfully enter to workplace or residence building premises, and may commit felony, theft or damaging a structure or asset, either at work or residence premises. |
| 13 | Intimidation and discrimination | Intimidation-Attempts by criminals and/or local armed militia and/or local government/informally organized forces to intimidate staff or extort the project workers or project affected persons of money/possessions. Scenario assumes limited fatalities but possible severe injuries.Discrimination-developing negative outlook against of their age, disability, ethnicity, origin, political belief, race, religion, sex or gender, language, culture and on many other grounds. |
| 14 | Abduction/kidnapping and hijacking  | Abduction of project workers or project affected persons by malign actors or organized criminal groups with the aim of terrorizing staff or extracting a ransom payment from the contractor or the government.Kidnapping-criminal offence consisting of the unlawful taking and carrying of a person by force or fraud or the unlawful seizure and detention of a person against his/her will. It may involve kidnapping staffs, workers, community members and ina worst scenarios children (e.g., South Sudan Murle kidnapped 275 children from Ethiopia, between 2015-2020.Hijacking- Hijack of vehicle/s with the intent to steal – scenario assumes possible fatalities as a result of hijack action. |
| 15 | Financial corruption | The abuse of entrusted authority (public or private) for illegitimate (private or group) gain. It compromises the institution’s capacity to perform its function in an impartial and accountable manner. |
| 16 | OHS risk to the security personnel | In addition, transmission of communicable diseases is also a concern including Covid-19 and Sexually Transmitted Diseases notably HIV/AIDS. Workers may also increase the rates of crime, social conflict and violence especially if they are unfamiliar with cultural norms in the areas where they are working. Construction activities may pose potential health and safety concerns for the inhabitants within the vicinity of works especially when construction is carried out near a village/community. Transport of materials, equipment and workers will use existing roads which may cause disruption or accidents resulting in injuries.Threats categorized as hazards are generally safety-related or linked to natural conditions. A threat that is described as a hazard is essentially one in which there is no deliberate intention to harm. Natural hazards like landslides and flooding, as well as human-made hazards such as e-waste should be considered when implementing EA-RDIP. More extreme natural hazards, such as earthquakes and volcanic eruptions, may also be of concern but potentially be unavoidable. Thought should thus be given to how these might be coped with. |
| 17 | Risk due to presence of security forces | The presence of security can result in risks to the community including undue use of force, inappropriate conduct to the community, increased risk of SEA/SH etc. |
| 18 | Terrorism | a method of coercion that utilizes or threatens to utilize violence in order to spread fear and thereby attain political or ideological goals. |

### 4.8.2. Key Security Threats-Specific to Sample Project Areas

As per the PAD, 5 priority fiber optic link points/Woredas (Adwa, Bameza, Halli, Gode and Dolo Odo) are identified under cross-border backbone network connectivity, and are linked to sub-component 1.1., Cross-border and backbone network connectivity. Under sub-component 1.2., Last mile connectivity including in borderland areas refugees/IDP and host communities are proposed to be covered. Two regional states, and four Woredas and one town are identified as IP Microwave points are identified. These link or connection points are Gambela (Dima Woreda), Somali (Aw-Bare Woreda, Kebribeya town, Dolo Odo and Bokolmayo Woredas).

#### 4.8.2.1. Afar Regional State

The recent war was conducted largely in towns and rural areas with dense civilian populations, a significant number of civilians have died, suffered physical and psychological injuries as well as sexual and gender-based violence as a direct result of acts of violence committed by parties to the conflict. The parties to the conflict include Tigray Forces and allied militia (in some locations including the Oromo Liberation Army (OLA)- aka “OLF-Shane”) on the one hand, and the security forces of the government of Ethiopia (Ethiopian National Defense Forces (ENDF) and allied security forces, Afar and Amhara security forces and allied militia) on the other.

The findings show parties to the conflict carried out indiscriminate attacks on civilians who are vulnerable in particular women, children, persons with disabilities and older persons.[[31]](#footnote-31) These attacks on civilians and civilian objects were committed in violation of the principles of distinction, necessity, precaution, and proportionality. By using civilians as human shields, conducting military operations from civilian homes and in urban areas, the parties have caused civilian deaths, physical injuries, and property destruction. Without including the extrajudicial killings, at least 403 civilians have died and 309 have suffered minor to serious physical injuries as a result of acts of violence in the context of the conflict.[[32]](#footnote-32)

Many civilians were displaced and suffered physical, mental, social, economic and other injuries following the expansion of the conflict into Afar and Amhara Regions. Insecurities resulting from the war and human rights violations including large-scale looting and destruction perpetrated by Tigray Forces were the main drivers of displacement from Afar and Amhara regions.

Separation from family members, inadequate humanitarian assistance including food, health services, clothing, and bedding; as well as shortages of sanitary pads and other specific supplies for women, children, older persons and persons with disabilities has aggravated the precarious situation of the most vulnerable IDPs.

The war has caused a grave humanitarian crisis in Afar, Amhara and Tigray Regions, significantly increasing the level of humanitarian need. While it is apparent that the ongoing conflict in Afar Region has impeded humanitarian relief services into Tigray Region, administrative and bureaucratic criteria and processes by federal and regional governments have slowed and limited the humanitarian relief.

Children were killed, subjected to SGBV, physical and psychological injuries, as a direct result of acts of violence taken by parties to the conflict. Children were exposed to traumatic experiences such as witnessing the killing, physical injury to or rape of close family members. The destruction of health and education facilities has resulted in a violation of children’s right to health and education. Beyond the social, economic, and psychological injuries, large-scale civilian displacement has denied children the protection they receive from their family members.

Persons with disability and older persons died, suffered physical and mental injury, as a result of violations committed by parties to the conflict. Older women were subjected to sexual violence. Older persons whose houses and property were destroyed suffered additional injury, trauma, and exposure to other socio-economic challenges, because they lost sources of financial support due to family members being killed or physically injured.

The widespread nature of the human rights violations detailed in the report[[33]](#footnote-33) and the large number of civilian populations affected also demonstrates that the task should not be left solely to the criminal justice apparatus. Accordingly, relevant national and international institutions should coordinate support to the Government in rehabilitation and resumption of health, education and other public facilities and services as well as relief services to IDPs and conflict affected populations.

Table : Calculated security risk value of Afar Regional State for EA-RDIP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat No.** | **THREAT TYPE** | **FREQUENCY** | **SEVERITY** | **IMPACT SCORE**  |
| **1** | Armed Robbery/Raid | 3 | 3 | 9 |
| **2** | Armed conflict between government and non-government forces | 3 | 5 | 15 |
| **3** | Theft of construction materials | 2 | 2 | 4 |
| **4** | Access blockage to some regions, cities or woredas | 3 | 4 | 12 |
| **5** | Risk of GBV/SEA/SH | 3 | 3 | 9 |
| **6** | Local conflict between ethnic groups and clans | 2 | 3 | 6 |
| **7** | Labor influx and human trafficking | 3 | 3 | 9 |
| **8** | Trespassing | 2 | 2 | 4 |
| **9** | Community protests | 2 | 3 | 6 |
| **10** | Unmet community expectation or where benefits sharing is perceiving to be lacking or unfair | 3 | 4 | 12 |
| **11** | Acts of violence | 2 | 4 | 8 |
| **12** | Burglary of work place/residence | 2 | 2 | 4 |
| **13** | Intimidation and discrimination | 2 | 2 | 4 |
| **14** | Abduction/kidnapping and hijacking  | 2 | 2 | 4 |
| **15** | Financial corruption | 3 | 4 | 12 |
| **16** | OHS risk to the security personnel | 3 | 3 | 9 |
| **17** | Risk due to presence of security forces | 2 | 3 | 6 |
|  | **Cumulative Rating** | **133/17=7.82** |

*Note:*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *High* |  | *Moderate* |  | *Low* |  |  |

#### 4.8.2.2. Gambella Regional State

The overall security situation in the Region remains unpredictable and volatile. The situation in Gambella has been very tense over the past year, due to unsolved ethnic tensions between the Anuak and Nuer population. Clashes between both groups have occurred on a regular basis creating security and access challenges for humanitarian partners. Among others, access to land and water for livelihoods (agriculture and pastoralism in particular) figure prominently as main sources of conflict. The region is vulnerable to cross-border incursions by the Southern Sudanese Murle and the Lou Nuer, who regularly raid cattle in remote woredas in the western part of the region.

On June 14, 2022, the Oromo Liberation Army (OLA), and the Gambella Liberation Front (GLF) militants entered and attacked Gambella town. After hours of long clashes, regional and federal security forces retook control of the city. The 13-page report by the Commission concludes that regional security forces extra-judicially killed 50 and injured 25 civilians who were suspected of ‘hiding firearms of the Oromo Liberation Army (OLA)’[[34]](#footnote-34).

The report further indicated that there had been looting and destruction of properties by the Oromo Liberation Army ( OLA), Gambella Liberation Front (GLF), regional state’s special forces, local militias, and affiliate youth groups in the town and its vicinities.

Just like the other regions of Ethiopia the SGBV practices are inherent and long-standing challenge in the region. The region has conservative social cultural practices that are patriarchal with entrenched power imbalance and gender inequality against women and girls. Most reported type of SGBV include, physical violence (mostly intimate partner violence), sexual violence (including rape), parents marry off adolescent girls from the age of 14 years with very low education completion rates.

Table : Calculated security risk value of Gambella regional state for EA-RDIP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat No.** | **THREAT TYPE** | **FREQUENCY** | **SEVERITY** | **IMPACT SCORE**  |
| **1** | Armed Robbery/Raid | 5 | 4 | 20 |
| **2** | Armed conflict between government and non-government forces | 4 | 5 | 20 |
| **3** | Theft of construction materials | 3 | 3 | 9 |
| **4** | Access blockage to some regions, cities or woredas | 3 | 4 | 12 |
| **5** | Risk of GBV/SEA/SH | 3 | 3 | 9 |
| **6** | Local conflict between ethnic groups and clans | 3 | 3 | 9 |
| **7** | Labor influx and human trafficking | 3 | 3 | 9 |
| **8** | Trespassing | 2 | 2 | 4 |
| **9** | Community protests | 2 | 2 | 4 |
| **10** | Unmet community expectation or where benefits sharing is perceiving to be lacking or unfair | 2 | 3 | 6 |
| **11** | Acts of violence | 3 | 4 | 12 |
| **12** | Burglary of work place/residence | 2 | 2 | 4 |
| **13** | Intimidation and discrimination | 2 | 2 | 4 |
| **14** | Abduction/kidnapping and hijacking  | 2 | 2 | 4 |
| **15** | Financial corruption | 2 | 3 | 6 |
| **16** | OHS risk to the security personnel | 3 | 3 | 9 |
| **17** | Risk due to presence of security forces | 2 | 3 | 6 |
|  | **Cumulative Rating** | **147/17=8.65** |

*Note:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  *High* |  | *Moderate* |  | *Low* |  |  |

#### 4.8.2.3. Somali Regional State

In December 2018, the general security situation in parts of the Somali region was volatile due to inter-communal clashes mostly located in Fanfan and some isolated incidents in other locations. No incident reports were received on other locations of intended return areas in the Somali region. The Ethiopian Defense Forces (EDF) was deployed to affected areas,needed. Apart from this, local groups of civilians are organized to play a role of military to maintain peace and security in the area.

On the first week of July 2022, Al Shabaab and Somali regional special forces engaged in multi-day clashes in Hargeleworeda in Afder zone in Somali region in Ethiopia, in addition to a couple of locations – Yeed and Ato – on the Somali side of the border. On 22 July, regional special forces besieged Al Shabaab militants in Holdhir area in Hulul in Hargele woreda, reportedly “destroying” the group (Somali Regional State Communication Bureau, 23 July 2022). At least 17 people, including three civilians and Ethiopian police officers, as well as over 100 members of Al Shabaab were reported killed during these clashes (FDRE Government Communication Service, 27 July 2022; VOA Amharic, 26 July 2022; Reuters, 22 July 2022). These incidents followed clashes between regional special forces and around 60 members of Al Shabaab a week earlier, on 14 July, during which an Al Shabaab commander was killed around Bula mountain in Elkare-Serer woreda in Afder zone. A few days later, the federal government announced the arrest of several Al Shabaab militants as they were allegedly planning to carry out attacks in Addis Ababa.

Attacks involving Al Shabaab are relatively rare in Ethiopia, despite a lengthy border with Somalia where the militant group is active. This is mostly due to the presence of Somali regional special forces, sometimes called by their Amharic term “Liyu Hayl” (for more details on this actor, see EPO’s Actor Profiles pages: Police Force of Ethiopia (2018) Liyu Police and Police Force of Ethiopia (2018)Somali Regional Special Forces), who are also deployed inside Somalia as part of the African Union Transition Mission in Somalia (ATMIS) (Long War Journal, 25 July 2022). Despite their effectiveness, Somali regional special forces have been accused of serious human rights abuses in both Somalia and Ethiopia (Human Rights Watch, 20 August 2018). ENDF soldiers are also present in Somalia, and more have been deployed to the border area since the latest round of clashes.

Internationally, a revived Al Shabaab threat also highlights the reliance of the international community on Ethiopian forces in combating radical Islamic groups in Somalia. As pressure has mounted on the Ethiopian government to address reports of human rights abuses committed by its troops in Tigray and Oromia, it is likely that it has felt a need to remind the international community of its historic contributions toward combating Al Shabaab in Somalia. The group’s incursion into Ethiopia has provided it with an opportunity to showcase its role in countering the Al Shabaab insurgency.

Nonetheless, the resurgence of political violence by Al Shabaab in Ethiopia is concerning. It highlights a continued trend of expansion by the group into a potentially receptive region of Ethiopia. Despite these concerns, reports of the defeat of Al Shabaab in Ethiopia demonstrate the capability of the Ethiopian security forces and their ability to address security concerns on the eastern border, which could boost much-needed support for the government throughout the country.

Situations such as early and forced marriages, female genital mutilation/cutting and domestic violence are frequent in the Somali region due to cultural norms and economic reasons. Girls have to assist parents in raising the younger siblings, participate in domestic chores and get married at an early age. Cases of rape and other sexual violence have also been reported in Jarar zone, whilst the highest rate of FGM/C is reported in Afder zone. There is a One-Stop-Centre in Jijiga to which SGBV survivors can report incidents. In areas, where One-Stop-Centres have not been established, survivors can report to the Bureau of Women, Children and Youth Affairs or its representation at the zone level.

Table : Calculated security risk value of Somali regional state for EA-RDIP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat No.** | **THREAT TYPE** | **FREQUENCY** | **SEVERITY** | **IMPACT SCORE**  |
| **1** | Armed Robbery/Raid | 3 | 4 | 12 |
| **2** | Armed conflict between government and non-government forces | 4 | 5 | 20 |
| **3** | Theft of construction materials | 3 | 3 | 9 |
| **4** | Access blockage to some regions, cities or woredas | 3 | 4 | 12 |
| **5** | Risk of GBV/SEA/SH | 3 | 2 | 6 |
| **6** | Local conflict between ethnic groups and clans | 3 | 3 | 9 |
| **7** | Labor influx and human trafficking | 3 | 3 | 9 |
| **8** | Trespassing | 3 | 2 | 6 |
| **9** | Community protests | 2 | 2 | 4 |
| **10** | Unmet community expectation or where benefits sharing is perceiving to be lacking or unfair | 2 | 3 | 6 |
| **11** | Acts of violence | 3 | 4 | 12 |
| **12** | Burglary of work place/residence | 2 | 2 | 4 |
| **13** | Intimidation and discrimination | 2 | 2 | 4 |
| **14** | Abduction/kidnapping and hijacking  | 2 | 2 | 4 |
| **15** | Financial corruption | 3 | 3 | 9 |
| **16** | OHS risk to the security personnel | 3 | 3 | 9 |
| **17** | Risk due to presence of security forces | 3 | 3 | 9 |
| **18** | Terrorism | 2 | 5 | 10 |
|  | **Cumulative Rating** | **150/18=8.33** |

*Note:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  *High* |  | *Moderate* |  | *Low* |  |  |

### 4.8.3. Key Security Threats-Risk matrix Summary

By multiplying the likelihood score with the frequency score a Risk Score/Impact score is generated for each threat scenario. Each threat scenario is numbered: see Table 14 below. Each threat scenario (represented by its number) is then plotted onto a risk matrix for each sample project regional state.

Table : Numbered list of security threats in sample regional states of EA-RDIP

|  |  |
| --- | --- |
| **Threat No.** | **THREAT TYPE** |
| 1 | Armed Robbery/Raid |
| 2 | Armed conflict between government and non-government forces |
| 3 | Theft of construction materials |
| 4 | Access blockage to some regions, cities or woredas |
| 4 | Risk of GBV/SEA/SH |
| 6 | Local conflict between ethnic groups and clans |
| 7 | Labor influx and human trafficking |
| 8 | Trespassing |
| 9 | Community protests |
| 10 | Unmet community expectation or where benefits sharing is perceiving to be lacking or unfair |
| 11 | Acts of violence |
| 12 | Burglary of work place/residence |
| 13 | Intimidation and discrimination |
| 14 | Abduction/kidnapping and hijacking  |
| 15 | Financial corruption |
| 16 | OHS risk to the security personnel |
| 17 | Risk due to presence of security forces |
| 18 | Terrorism |

#### 4.8.3.3. Afar Regional State

Table : Afar Regional State-Risk Matrix

|  |  |
| --- | --- |
| **Risk Matrix** | **Impact Score-Frequency x Severity** |
| **Severity** |
| **Negligible-1** | **Minor-2** | **Moderate -3** | **Severe-4** | **Critical-5** |
| **Likelihood /Probability of Threat** | **Very likely****(75%+)/5** |  |  |  |  |  |
| **Likely****(55-74%)/4** |  |  |  | **2** |  |
| **Moderately likely****(40-54%)/3** |  |  | **1,5,16** | **,4,7,10,15** |  |
| **Unlikely****(25-39%)/2** |  | **3,8,12,13,14,17** | **6,9** | **11** |  |
| **Very unlikely****(-24%)/1** |  |  |  |  |  |

The result in Afar regional state reveals that there is a moderate rating value/12 for 5 indicators/security threat types including ; access blockage to some regions, cities or Woredas; labor influx and human trafficking; unmet community expectation or where benefit sharing is perceived to be unfair; and arrest and detention. Besides it has scored moderate rating/9 in the case of armed robbery, risk of GBV/SEA/SH, and financial corruption. The rating for armed conflict between government and non-government conflict is 16 or which is very high. Furthermore, it has registered a moderate rating/8 on acts of violence and moderate rating value/6 on local conflict between ethnic groups and clans. The remaining six indicators are rated with a security threat value of low/4.

#### 4.8.3.3. Gambella Regional State

Table : Gambella Regional State-Risk Matrix

|  |  |
| --- | --- |
| **Risk Matrix** | **Impact Score-Frequency x severity** |
| **Severity** |
| **Negligble-1** | **Minor-2** | **Moderate-3** | **Severe-4** | **Critical-5** |
| **Likelihood /Probability of Threat** | **Very likely** **(75%+)/5** |  |  |  |  |  |
| **Likely****(55-74%)/4** |  |  |  |  | **1,2** |
| **Moderately Likely****(40-54%)/3** |  | **10,15,17** | **3,5,6,7,16** | **4,11** |  |
| **Unlikely****(25-39%)/2** |  | **8,9,12,13,14** |  |  |  |
|  **Very Unlikely****(-24%)/1** |  |  |  |  |  |

The result indicates Gambella has registered substantial rating value in the case of armed robbery and conflict among government and non-government forces, which are 20 . Besides it has scored moderate rating/12 in the case of access blockage to some regions, cities or Woredas, acts of violence, and it has registered a moderate rating/9 on five security threat types. The rating for the remaining three indicators is moderate/6 and for the other five indicators is low.

#### 4.8.3.3. Somali Regional State

Table : Somali Regional State-Risk Matrix

|  |  |
| --- | --- |
| **Risk Matrix** | **Impact Score-Frequency x severity** |
| **Severity** |
| **Negligible-1** | **Minor-2** | **Moderate-3** | **Severe-4** | **Critical-5** |
| **Likelihood /Probability of Threat** | **Very likely****(75%+)/5** |  |  |  |  |  |
| **Likely****(55-74%)/4** |  |  |  |  | **2,18** |
| **Moderately likely****(40-54%)/3** |  |  | **3,6,7,15,16,17** | **1,4,11** |  |
| **Unlikely****(25-39%)/2** |  | **9,12,13,14** | **5,8,10** |  |  |
| **Veryunlikely****(-24%)/1** |  |  |  |  |  |

The finding in Somali regional state shows that there is a very high rating value/20 armed conflict between government and non-government forces and terrorism. The second highest rating value which is moderate/12 is associated with armed robbery, access blockage to some regions, cities or Woredas and acts of violence. Besides it has scored moderate rating/9 in the case of theft of construction materials, local conflict, labor influx and human trafficking, financial corruption, OHS risk to the security personnel and risk due to the presence of security personnel. Furthermore, it has registered a moderate rating/6 on risk of GBV/SEA/SH, trespassing and unmet community expectations. The remaining four indicators are rated with a security threat value of low/4.

EA-RDIP is assessed overall as medium security risk of the sampled three regional states which are included in the project. The analysis identified 17 key security risks in project regions (Afar,Gambella having an overall rating 0 Critical, High risk, Substantial and low and negligible /very low/risks, and 3 medium risks. The overall rating for the sample regional states is moderate, such as; Afar 7.65/moderate, Gambella 8.4/moderate and Somali 8.2/moderate. The average rating of the summation of the regional states is 24.25/3=8. Thus, the combined overall rating of the sample regional states is 8/moderate.

## 4.8. Mitigation Measures

Potentially security risks and impacts identified for the EA-RDIP can be avoided, minimized and mitigated in various ways. The ESMF proposes potential mitigation measures and instruments for all anticipated risks and impacts. The following are the potential measures to specifically address the security risks and impacts:

Table : Summary of potential security threats and mitigation measures

|  |  |  |
| --- | --- | --- |
| ***Security Risks Identified*** | ***Proposed Mitigation Measures*** | ***Responsible Body*** |
|  Armed robbery | * Enhanced Information and Communication platforms between Woreda program implementation unit and local public security forces
* Increased coordination and information sharing on potential security risks from armed groups operating in the area with other trusted public security actors
* Thorough risk assessment and contextual analysis, in addition to routine measures (counter-terrorist search, hostile surveillance and reconnaissance detection and convey escort/protection if applicable), necessary for detecting armed groups presence in the area
* Suspension of program activities in program areas (located within 25 Km of the incident’s place), presence of armed groups is detected.
* HEAT training for staff at most riskn/exposed to high risk
 | * PIU
* Local and regional officials
* Local and regional security officials
* Contracted firms
* Program security focal person
 |
| Armed conflict between government and non-government forces | * Conducting socio-economic conflict analysis to understand the root cause of border conflicts in program implementation areas.
* Map out’ warring factions, individuals, organizations and strategies that could help resolve border conflicts
* Early identification and management of conflict Intensifying factors: ethnic conflict, recent violence, historic animosity, weakness of claimant groups (to control potential break-outs
* Identify conflict ‘warning signs’. Communities can make a list of warning signs that would be evidence of increasing border tensions within or between communities
* Hostile environment awareness training (HEAT) for those staff most at risk of exposure to this risk. Supported by better intervention plan
 | * PIU at the MInT
* Contracted firms
* Public security Personnel
* Private security personnel
* woreda peace and security bureau
 |
| Theft to construction materials at a project site | * Site access control: guidelines for security personnel on how to interact with community members seeking access to Program site or raising a concern (for example, training on the grievance mechanism and Code of Conduct).
* Use of physical security personnel.
* premises fencing especially materials areas, storage areas like construction sites
* Establish formal and consistent reporting and communications mechanisms with local police and other security related stakeholders.
* Strengthen physical security measures (fence, gate check, store lock)
* Assign additional security guard in collaboration with local administration
* Assessment and health and safety protocols.
* Manned guarding: Entry and exit monitoring; Locking away and security marking of plant, tools and equipment, hazardous materials, etc.
* Managing and operating technology which supports security, such as setting alarms and automated systems.
* Training on potential hazardous materials on site, proper equipment to report events (telephone, radios, etc.),
* Proper training and equipment to deal with potential events due to incurrences into construction site (e.g., fires, release of hazardous materials).
* Training needed for construction workers, community workers and security personnel with each training designed for the type of worker.
 | * Woreda EA-RDIP program coordinator
* program Security focal person/coordinator
* Local police
 |
| GBV/SEA | • Fully implement sanctions contained in the GBV Action Plan (Please refer GBV Action Plan Annex 6 on the ESMF).-Strengthen treatment and referral pathways for GBV/SEA survivors-Raise awareness on GBV/SEA protocols for the Project in line with LMP -Provide separate ablution facilities for men and women at the workplace -Ensure proper lighting on the compounds* Fully implement sanctions contained in the GBV Action Plan (Please refer GBV Action Plan Annex 6 on the ESMF).
 | * Federal, regional, woreda PIU, and administrators
* Contractors and sub-contractors
* Implementing Agencies,
* Security players in the devolving government structures
 |
| Local conflict occurs between ethnic groups and clans | * Ensure PIU recruits, equips, and trains security forces consistent with Program SMP
* Conducting socio-economic conflict analysis to understand the root cause of border conflicts in program implementation areas.
* Map out’ individuals, organizations and strategies that could help resolve border conflict
* Early identification and management of conflict Intensifying factors: ethnic conflict, recent violence, historic animosity, weakness of claimant groups
* Monitoring and defining potential triggers for suspension of activities and evacuation of project personnel
* .Hostile environment awareness training (HEAT) for those staff most at risk of exposure to this risk
 | * PIU
* Public Security Officials and Army Commands
* Local Political Officials
 |
| Labor influx and women trafficking | * Communicate expectations regarding appropriate conduct, together with disciplinary measures;
* Depending on the nature of the project, adoption of a formal code of conduct.
* Prevent any kind of involuntary or compulsory labor, such as indentured labor, bonded labor, or similar labor-contracting arrangements.
* No trafficked persons will be employed in connection with the project.
 | * Federal, regional, city PIU, and administrators
* Contractors and sub-contractors
* Implementing Agencies,
* Security players in the devolving government structures
 |
| Trespassing | * Cultivate strong community relationships and information sources
* Coordination and deconfliction with Ethiopian Defence Forces and regional armed forces
* Ensure pre-departure checks are carried out ahead of all journeys
* Recruit dedicated security coordinator to oversee mitigation measures and incident management
 | * PIU
* Public Security Officials and Army Commands
* Local Political Officials
 |
| Community protest | * Liaison with all interlocutors at all levels including government security forces, civil society, other parties to the conflict and project beneficiaries
* Ensure minimum physical security measures are in place for Staff accommodation when not residing in a Humanitarian Hubs.
* IDs provided for identification of staff/project personnel
* Where private guards are present, training on active and hostile surveillance and managing crowds
* Evacuation/relocation plan in place for EA-RDIP II staff
 | * PIU
* Public Security Officials and Army Commands
* Local Political Officials
 |
| Unmet community expectations, or where benefit sharing is perceived to be lacking or unfair | * Strictly adhere to the provisions set in Project Implementation Manual
* Accessible and repeated community members consultations composing both program participant ,non-participant community members and local administration representatives
* Establish and strengthen locally accessible program grievance redressing/ handling mechanism.
* Designing a program membership arrangement that permits new membership opportunities vis-à-vis with certain commitment requirement
 | * PIU
* Program social safeguard coordinators
* Woreda/local administration n bureau
 |
| Acts of violence | * Minimize on site cash storage, keeping petty cash amounts.
* Access control procedures in place as per areas SRM.
* Security briefings and training.
* Liaison with interlocutors including government security forces
* Incident reporting process that should include local authorities
* Staff constant advice on maintaining low profile
* Security staff accompanying missions, where deemed necessary by a security risk assessment.
 | * PIU at the RPIU
* Contracted firms
* Public security Personnel
* Private security personnel
* Woreda peace and security bureau
 |
| Burglary of workplace/residence | * Access control in place at all sites, as far as reasonably practicable
* Use of unarmed guards/ watch people at project sites
* Asset management procedures, including inventories
* Secure storage of assets, such as warehousing, as outlined in the SOPs
* Seek insurance for high value items
* Recruit dedicated security coordinator to oversee mitigation measures and incident management
* Cultivate strong culture of incident reporting and follow-up
 | * Woreda EA-RDIP II project coordinator
* program Security focal person/coordinator
* Local police
 |
| Intimidation and discrimination | * Constant engagement with community leaders in EA-RDIP II operational areas.
* Liaison with interlocutors including government security forces
* Security briefings and adhoc training to raise situational awareness among personnel
* Incident reporting process that should include local authorities
* Staff constant advice on maintaining low profile
* Security staff accompanying missions, where deemed necessary by a security risk assessment.
* Relocation plan in place for EA-RDIP II and MInT staff
 | * Federal, regional, Woreda PIU
* Contractors and sub-contractors
* Implementing Agencies
* Security players in the devolving government structures
* Regional and Woreda Administration
 |
| Abduction/Kidnapping and hijacking: | * Use of physical security personnel,
* Ensure consistent reporting and communications mechanisms with public security forces and other stakeholders.
* Staff should avoid travel in darkness; only using trusted drivers / ; not set patterns and routines; keep in pairs or teams at all times.
* Local knowledge of the program/subproject area and operational context must be maintained by staff at all times.
* Seek information from project security focal person and clearance from PIU coordinator.
* 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.
* SRAMP should be made available to all staff and appropriate training conducted.
* Never fight back when apprehended with armed people
* Do not try to argue or make provocative comments.
* Do not stare or make eye contact with the kidnappers.
* HEAT training for at risk staff.
* The client shall develop a workable Kidnap and Ransom policy
 | * Federal, regional, woreda PIU
* Contractors and sub-contractors
* Implementing Agencies
* Security players in the devolving government structures
* Regional and Woreda Administration
 |
| Financial corruption | * Staffing reforms promote competition, performance/merit based career structures.
* Disclosure of assets
* Transparent appointment of qualified administrative leaders (and selection of political leaders)
* Ring-fencing finances of utilities, separation of roles between local government and utilities
* Support for improving integrity of business (professional associations, codes of conduct)
* Demonopolizing operations and maintenance
* Financial and technical audits and reporting
* Performance-based contracts with defined minimum standards
* Transparency in operations and management
* Citizen role in oversight
* Benchmarking utility performance Small/informal providers
* Improve interface between formal and informal
* Legitimization
* Formal bulk supply, pricing, competitive tenders for franchises
 | * City EA-RDIP II project coordinator
* program Security focal person/coordinator
* Local police
 |
| OHS risk to the security personnel | -Further reference shall be made to the relevant WBG EHS Guidelines to manage OHS risks to security personnel.-Conduct regular training and awareness project focused on the key and relevant content of international and national guidance, the ESMP, Code of Conduct, accident and incident reporting, accident root cause analysis and remedial measures, projects for project workers, community and IAs;Environmental and Social Clauses for Contractors Consultation (it will be included in bids and contractors’ contracts)Adhere to Hazardous material and Wastes Management set out in the ESMFAdhere to Labor Management Procedures (LMP).Adhere to Liquid and Solid Waste Management Guideline prepared for EARDIP II.Ensure ESHS/OHS provisions are incorporated in the bidding documents and contract agreement for construction.Design and implement a contingency plan/site-specific OHS plan to manage potential accidents or natural disasters in situations of normal operation as well as under state of emergency, based on the vulnerability of the country to natural disasters; the plan must include an Occupational health plan and be approved by the Ministry of Health/MInT ESHS or OHS unit.Train personnel and workforce in the implementation of the contingencyPlan/site-specific OHS plan.Ensure that waste management is operable to reduce the fuel element for fireEnsure a fire alarm/smoke alarm system is operable within the sitesConduct regular Environmental and Social Monitoring and audit (the security monitoring will be included in regular E&S monitoring).Conduct regular emergency drills at project sites in coordination with relevant local authorities.Evaluate potential exposure toworkers against the reference levels developed by the International Commission on Non-Ionizing Radiation Protection (ICNIRP).Take into account security personnel’s perception about Electromagnetic Fields (EMF) by consulting with the local community after the sitingprocess of antenna towers.Limit public access to antennae tower locations.Levels of EMF in workplaceIdentify potential exposure in theworkplace Train workers in the identification of occupational EMF levels and hazards Identification and establishment of safety zones to differentiatebetween work areas and public areasDevelopment and implementation of an EMF safety program, as set out by the WB’sEHS Guidelines for Telecommunications | * Federal, regional, city PCU
* Contractors and sub-contractors
* EPA in the devolving government structures
* Regional and City Administration
* Labor offices
* E and S specialist and Focal persons
 |
| Risk due to presence of security forces | * Effecting Contractual arrangements with all involved security guards hence provide clear instructions on expected code of conduct.
* Induction training to recruited security personnel, covering topics like, proportionate use of force, what constitutes sexual harassment, GBV, and program’s asset management system
* Documented disclosure of program’s policy on firearm holding, utilization and disciplinary measures for breaches on code of conduct
* Establish accessible means of receiving and reporting incidents and allegations regarding misconducts by security personnel
* Adhere to WB Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel as well as other good international practices and standards.
 | * PIU
* Contacted private security company
 |
| **Other Common Security Threats-Not Rated by this Assessment** |
| Insecure road transportation including access blockage to some project regions and Woredas | * Enhanced Information and Communication platforms between Worreda program implementation unit and local public security forces
* Increased coordination and information sharing on potential security risks from armed groups operating in the area with other trusted public security actors
* Thorough risk assessment and contextual analysis, in addition to routine measures, necessary for detecting armed groups presence in the area
* Suspension of program activities in forest areas, presence of armed clash is detected.
* Armed escorts, where appropriate, plus HEAT training for staff
 | * PIU
* Contracted firms
* Public Security Officials
* Army Commands
* Political Officials
 |
| Workplace injuries/safety risks, including road safety | * Strictly apply the program LMP; purchase and supply of PPE materials; enforce the workplace safety features as per the OHS plan.
* Awareness raising training on work-place safety cultures, including road safety
* Establishment of first-aid corner or mobile first-aid boxes
* Basic first-Aid training to program workers and Forest management cooperatives members
 | * PIU, RPIU and Woreda level focal person
* Regional and Woreda security office
* Woreda administration
* Security management team
* Contractors
* Consultants
 |
| Risks related to presence of mobile plant and vehicles, risks related to musculoskeletal health and load loading, and risks related for exposure to chemical agents.  | 1. ***Measures related to mobile plants and vehicles risks***
* Access to vehicles would be limited to sealed and stabilized areas, as far as practicable, to reduce dust generation.
* Ensure that all vehicles entering and leaving the site and carrying a load that may generate dust are covered at all times, except during loading and unloading. Any such vehicles shall be covered or enclosed in a manner that will prevent emissions of dust from the vehicle at all times.
* Movement of vehicles, machinery and equipment will be through designated corridors.
1. ***Measures to exposure to chemical agents***
* Maintenance schedules including engine tuning, filter cleaning, etc. for construction equipment and vehicle will be implemented according to manufacturers’ specifications.
* Chemicals shall be stored in a shaded, cool and well-ventilated area (as per chemical storage requirements). This will help ensure that no fumes of gases are seeping into the surrounding air.
* Onsite repair, maintenance, oil change, cleaning, and washing for the plants, equipment, vehicles, concrete truck mixers, etc. is prohibited.
1. ***Measures related to muscloskeletal healt and load loading***

Elimination, substitution, engineering controls, administrative controls and use of personal protectiveA three-tier hierarchy of controls is widely accepted as an intervention strategy for reducing, eliminating, or controlling workplace hazards, including ergonomic hazards. The three tiers are:1. Elimination

Elimination, or physically removing a hazard from a workplace, is the most effective stage of the hierarchy of controls. When hazards are eliminated or removed from a work environment, they no longer have the potential to negatively impact employees. Though it’s conceptualized as the most effective stage, elimination is also typically the most challenging to implement. Doing so can be costly and require major overhauls in preexisting workplace processes.Examples:• Redesign a process to eliminate the use of hazardous equipment or product• Perform tasks at ground level rather than working high above ground• Store goods at lower heights so workers don’t have to climb tall heights and risk fall injuries or fatalitiesb. SunstitutionSubstitution, or replacing a hazardous item or activity with something less hazardous, is the second-most effective stage of safety control. Substitution serves a similar purpose to elimination, as it removes a hazard from the workplace or decreases the potential for the hazard to negatively affect employees. If a workplace process is still in its design or development phase, substitution can be an inexpensive and streamlined method for managing a hazard.Example:• Replace a caustic cleaning agent with a non-toxic alternative• Substitute a solvent-based paint with water-based paint• Use a non-silica abrasive material instead of sandblasting1. Use of engineering controls

It referes to a method of managing OHS hazards, such as incidents, injuries, and illnesses by isolating employees/workers from the hazard(s). Engineering controls, or designing purposeful solutions that physically separate employees from hazards, are the third-most effective stage of safety control. Many organizations favor engineering controls to remove the hazard at the source, rather than after an employee comes into contact with a hazard. It’s important to note that while engineering controls can sometimes be costly to implement, they typically result in lower overall operating costs due to the new safety features.The preferred approach to prevent and control muscloskeltal health and load loading is to design the job to take account of the capabilities and limitations of the workforce using engineering controls (e.g., …). Examples: • Place barriers around fans and other loud machinery• Fence around dangerous high-voltage equipment• Install guardrails at worksites that are high above ground1. Use of administrative controls (changes in work practices and management policies)

Administrative control strategies are policies and practices (such as ….) such as; operating procedures, work duration protocols and workplace signage protocols that reduce muscloskeletal health and load loading risk but they do not eliminate workplace hazards. Although engineering controls are preferred, administrative controls can be helpful as temporary measures until engineering controls can be implemented or when engineering controls are not technically feasible. Examples:• Limit the time a worker is exposed to a hazard• Create written formalized operating procedures• Install signs, labels and alarmse. Use of personal protective equipment (PPE)PPE, physical equipment worn or used by employees while they perform their work, are the fifth- or least-most effective stage of the hierarchy of controls.PPE generally provides a barrier between the worker and hazard source. Respirators, ear plugs, safety goggles, chemical aprons, safety shoes, and hard hats are all examples of PPE. Whether braces, wrist splints, back belts, and similar devices can be regarded as offering personal protection against ergonomic hazards remains an open question. Although these devices may, in some situations, reduce the duration, frequency or intensity of exposure, evidence of their effectiveness in injury reduction is inconclusive. In some instances, these devices may decrease one exposure but increase another because the worker has to “fight” the device to perform the work. Examples:• Eye and face protection (goggles and masks)• Head protection (hard hats)• Foot and leg protection (foundry shoes)• Hand and arm protection (chemical-resistant gloves)• Body protection (hazmat suits)* • Hearing protection (earplugs)
 | * PIU, RPIU and Woreda level focal person
* Regional and Woreda security office
* Woreda administration
* Security management team
* Contractors

Consultants |
| Delay in procurement and public work and PPE material supply | 1. Assess and use alternatives including local markets

Coordination with government security bodies incase their engagement and support is needed while transporting construction materials from central market place and to construction sites | * PIU, RPIU and Woreda level focal person
* Regional and Woreda security office
* Woreda administration
* Security management team
* Contractors
* Consultants
 |
| Security-posed GBV Risks | * Strictly adhere to the provisions set out in the Program GBV Action Plan developed as part of the ESMF.
* Awareness-raising/training for security personnel (both private and public) on GBV.
* Awareness-raising training for women and local community members
* Grievances that deal with gender-related allegations must be handled very carefully, with respect for the confidentiality of the complainants, survivors and their families.
* working together, referrals and collaboration with Women and social affairs bureau
 | * PIU
* Contracted firms
* Public/government Security officials
* Woreda Women and Social Affairs bureau
 |
| Incident to project staff and project workers including physical beating and sexual harassment and GBV-by Security personel  | -Awareness creation on GBV and social harassment for communities 1. -Limit frequency of field travel to security risk areas
2. -Access updated information on security issues before any movement in to security risk areas
3. -Induct security personnel on the project’s CoC
4. -Ensure contracted security personnel sign the CoC
5. -Strengthen treatment and referral pathways for GBV/SEA survivors
6. -Raise awareness on GBV/SEA protocols for the Project in line with LMP and the ESF
7. -Provide separate facilities for men and women at the workplace
8. -Ensure proper lighting on work sites
9. -Fully implement measures and sanctions contained in the GBV/SEA/SH AP.
10. -Report to and get preventive support from higher security officers (police and regional special force)
* Adherence to requirements of the SEP, GBV/SEA/SH AP, LMP, GRM
 | * PIU, RPIU and Woreda level focal person
* Regional and Woreda security office
* Woreda administration
* Security management team
* Contractors
* Consultants
 |
| Impacts from deployment of public or private security personnel | * Effecting Contractual arrangements with all involved security guards hence provide clear instructions on expected code of conduct.
* Induction training to recruited security personnel, covering topics like, proportionate use of force, what constitutes sexual harassment, GBV, and program’s asset management system
* Documented disclosure of program’s policy on firearm holding, utilization and disciplinary measures for breaches on code of conduct
* Establish accessible means of receiving and reporting incidents and allegations regarding misconducts by security personnel
 | * PIU
* Contracted private security company
 |

# 5. Security Management Plan

This document is the Security Management Plan for EA-RDIP project. This document is intended to be a live, working document for the duration of the project implementation staffs and contract with the MInT/PIU of the proposed EA-RDIP project. It will be regularly reviewed and the content the narrative will be updated to reflect changes of note throughout the contract time. The document describes how MInT and the PIU manages project employees, community, properties of the contractor as well as the society’s security which is according to Ethiopian Government security practice and specifies any additional or different application of controls, specifically required to the nature of contactor’s services to the MInT/PIU and security nature of the project area.

## 5.1. Purpose of the Security Management Plan

The purpose of the Security Management Plan (SMP) is as follows:

* Define the scope and boundaries of the EA-RDIP project Security Management System;
* Document commitment by MInT’s/PIU’s management to a fit-for-purpose of project security management system;
* Document roles and responsibilities within MInT/PIU for the project security management system;
* Description of the major elements governing the implementation and operations of the project security management system that is required for compliance against World Bank Environmental and Social Standards (ESSs).

Therefore, MInT/ security manager or project coordinator/his or her designate shall:

* Document and keep this SMP and update it during EA-RDIP-project implementation;

 Evaluate the actual effectiveness of security mitigation options post-incident after exercises;

* Ensure that the prioritized security risks and impacts are taken into consideration in establishing, implementing this security management plan (SMP); and
* Evaluate the effectiveness of security risk controls and mitigation measures quarterly.

## 5.2. Objectives of the SMP

The Security Management Plan is designed to protect against and mitigate security risks at the project that could threaten communities, employees, facilities, and progress of EA-RDIP implementation. It provides direction, organization, integration, and continuity to the project security program.

The specific objectives of the Security Management Plan are the following:

(a) Identification and assessment of security risks include an analysis of contextual factors that could cause or exacerbate human security risks in the project area.

(b) Set the Processes of identification of different security requirements

(c) Identify the decision-making processes of MInT and minimum conditions for project implementation

(e) Identify the role and responsibilities of the different parties

(f) Sets out the operation polices, standards and institutional arrangements for the implementation of the SMP

(g) To estimate the cost of the potential impact and its implication on the future operation;

(h) Develop necessary SOPs (please see Annex 2), Crisis Response Protocol and security concept documents based on immediate needs; and

(i) Undertake security, risk and safeguard trainings with relevant staff

## 5.3. Scope of the SMP

This SMP define the content and structure of the EA-RDIP project security management plan. It will also address the requirements for staff, processes, documentation, technology and physical facilities needed to meet the specific physical and personal security, governance and assurance requirements of the WB and document how these additional requirements are to be added to the MInT’s environmental, social and occupational safety.

##  5.4. Security Management Plan Governance

This security management plan will be prepared inline to the requirements of WB ESF, more specifically as per the requirements of Environmental and Social Standard 1 (Assessment and Management of Environmental and Social Risks and Impacts), Environmental and Social Standard 2 (Labor and Working Conditions) and Environmental and Social Standard 4 (Community Health and Safety) and the Ethiopian Labor Proclamation (proclamation No 1156/2019). Also, the relevant WBG EHS Guidelines is considered in preparing the security management plan.

## 5.5. Overview of Security Management Plan

**Potential security risks of the Project (internal and external):** Project target areas and specific project sites present different levels of insecurity and safety problems based on the security contexts and the extent of security management measures in place. It is important to undertake security risk assessment on an ongoing basis to inform mitigation measures. The purpose of security assessment is to determine and assess areas of exposure to insecurity in project workplace. For additional information, please see section 4.5.1 of the SRA of this document.

The OHS risks to security personnel include (i) risks related to traffic safety while traveling outside of the site and within the site, (ii) risks from unsafe ingress and egress to the site, (iii) falling into open excavations while working near them, (iv) risk of fall from heights such as watch towers, (v) exposure to noise, vibration, and dust emission from the work area, (vi) risks from working close of electricity/energy sources, (vii) fall, slip, and trip risks due to poor housekeeping on the site, (viii) biological hazards such as COVID-19, STDs, and pathogens from wastewater and solid waste in the work area, (ix) Physical hazards from prolonged exposure to weather (heat, cold, rainfall, etc), (x) psychological stress, burnout and health effect due to the demanding nature of the work including working irregular hours, (xi) risks associated to preparedness and response in emergency situations resulting in bodily injuries and fatalities from crimes, violence, firearm accidents, etc., (xii) risks related to presence of mobile plant and vehicles, (xiii) risks related to musculoskeletal health and load loading, (xiv) risks related for exposure to chemical agents, and (xv) Risks from exposure of all OHS hazards identified for project works (please see the Labor Management Procedures for detailed OHS risks).

 **Project Security Risk Management Capacity:** Security Risk Management for the project lies under the oversight and responsibility of the project coordination unit at federal, regional and woreda level. The PIU, RPIU and Woreda level focal person will work closely with the regional and local government security bodies under the overall direction, supervision and control by the government existing administration. Accordingly, the project will utilize existing government security structures of implementing sectors at federal, regional, city levels. Relevant focal persons will be delegated at federal and regional levels to facilitate communications related to security concerns together with the project coordinator. Overall, the security management responsibility falls to the project coordinator and he/she may delegate to a project security manager as needed.

 It is anticipated that the project will not have security involvement over and above the
existing government arrangements. The institutional arrangement for SMP is presented on section 5.7., of this document. The major scenarios that may require security involvement are:

- The contractor works at specific project sites located near to the areas where law enforcement operation is undertaking

- Workers involved in the distribution of innovative technologies and different public work inputs.

- The material supply activities by private suppliers specifically in to insecure sites

- The project staff movement for the purpose of technical support, follow up monitoring and evaluation

- Project resource and construction materials temporary stored at construction site and

- Project vehicles in conditions that they may be exposed to non-government armed forces

As part of this SRA and SMP general security risk measures have been developed. However, at this stage the specific sub project site and activity to be financed by the project is not known. Hence, by the time the specific sub project site and each activity is known, a site and activity-specific risk assessment which, in turn, will guide the security measures to be adopted will be conducted. The project coordinator and security focal persons will be responsible for this. Insecure project sites and activities may require the presence of public security personnel, which most likely to be arranged by the region, *Woreda* and kebele government to accompany the overall project operation, material supply and staff movement.

## 5.6. Security Management Procedures for EA-RDIP

 The SRM process is an approach to evaluate security risks to ensure that a harmonized
threat and risk analysis leads to effective security decision-making and to the implementation of SRM measures. SRM measures are identified after specific threats and risks are identified so that mitigation or prevention measures are proposed for implementation. SRM measures may include training and awareness creation, information, situation updates, physical improvements to facilities or procedural changes. SRM measures need to be linked to the preceding security risk assessment assisting to reduce either the likelihood or the impact of an event. EA-RDIP will use the following risk management procedures while implementing the project operation in identified security potential areas.

1. Training and awareness creation;
2. Management of site work and staff movement
3. Use of Government security personnel
4. Equipment and project assets
5. Physical security
6. Response to different security alert levels (see Annex 1)
7. Suspension of activities
8. Emergency preparedness and response.

## 5.7. Oversight and Security Management

The responsibility for overseeing security risk management of EA-RDIP operation will be vested on the federal, regional and *Woreda* Project Area Focal Person/PAFP and contractors are responsible to ensure the safety and security of contracted workers and construction materials at sub project construction sites including reporting on any security concerns occurred at construction sites. The overall responsibility for overseeing project security rests on project coordinator and security focal person (Security Manager) at federal level and security focal persons for each of the regions. In collaboration with administrative bodies, the PAFP at all levels will be responsible for coordinating the overall project management through the existing government structure in fulfilling security safeguards requirements. Specifically, the PAFP will be responsible for:

- Undertaking site and activity specific security risk assessment and implementation of this Security Risk Management Plan;

- As part of sub-project screening, undertake security risk assessment and recommend mitigation measures;

- Ensure that security mitigation measures are included in sub-project ESMPs;

- Monitor potential security risks on sub-project sites together with the local government

- Initiate response procedures based on the security risk alert level (Annex 1 provides different security alert states and potential triggers).

- Provide training for concerned stakeholders to mitigate social risks of project workers and equipment including security risks;

- Ensure that project Grievance Redress Mechanism (GRM) established for the project and implemented and that project workers are informed about the GRM procedure;

- Report periodically to the World Bank on the implementation of the SRA and SMP.

In order to guide the overall activity of SMP, the organizational chart for the implementation of the SMP is present on the figure below:

Figure 5.7: Organizational responsibility chart for the implementation of security management plan.

##  5.8. Communication Protocols

Standard telecommunication connection facilities, which are within the scope of the project, will be the main means of communication method to be used during the implementation of this SRA and MP. This includes office telephone, mobile phone, and email, and fax communications. In case of remote areas where it is difficult to access the normal network and emergency cases including travel to field locations, the project will use other methods of communication (i.e. GSM & sat phone/VHF radio) through fulfilling the required country’s security requirements. Virtual communication options with RPIU and Woreda project coordination team will be strengthened during restrictions of movement.

## 5.9. Grievance Redress Mechanism

To extent possible, the SMP will adopt the Project Grievance Redress Mechanism in managing the security related grievances. The security manager shall engage the relevant project personnel to ensure security personnel grievances are included in the Project GRM and Stakeholder Engagement Plan, and work with public security leaders to integrate the project GRM with internal procedures. Key areas of emphasis will be on the following steps:

**Establish a grievance mechanism to receive security-related concerns or complaints:** It is important to have a structured and accessible process for receiving and responding to security-related complaints and to ensure that affected community members are aware of it. In general, concerns may come from a wide range of sources including communicated directly to Community Relations staff, kebele level-compliant handling committee, through a hotline telephone number, via tip boxes outside the program site, and suggestion boxes placed at sector bureau which are being involved in program implementation.

**Clarify reporting requirements and structure:** Good procedures normally specify which type of security-related allegations and incidents should be reported, to whom, and in what time frame. Complaint handling Procedures should clearly identify both the person(s) responsible for accepting and processing allegations or incidents, and escalation hierarchy to management.

 **Develop inquiry protocols:** In addition to a routine process for recording all incidents, more serious incidents or allegations related to security personnel conduct may require a more in-depth inquiry to determine whether policies and procedures were strictly followed and if any corrective, disciplinary, or preventive actions are warranted.

### 5.9.1. Key Steps in Security-Related GRM Process

 Every allegation or incident related to security should be assessed, regardless of whether in a low-risk or high-risk context. The level of depth and detail of inquiry should flow from the seriousness of the allegation or incident. The steps involving the GRM process are further discussed as follows.

 **Step One:** **Record the incident or allegation:** All incidents and allegations should be recorded, whether they come from an incident report, the grievance mechanism, or any other formal or informal means of communication. Serious allegations and incidents should be reported to senior management within the same day acts committed. Potentially criminal wrongdoing such as theft, rape/attempt of rape, carjacking, GBV, fire break-out should be reported to the relevant authorities within 24 hours. Annex 4 provides Sample Incident Report Summary Template.

 **Step Two: Collect information promptly:** Information should be collected as early as possible following an incident or receipt of an allegation. This may include noting details related to the circumstance, individuals involved, location, timing, and so forth, and taking statements and/ or photographs where relevant.

 **Step Three: Protect confidentiality:** PIU is advised to consider confidentiality measures to protect alleged victims, witnesses, and/or complainants—for example, identifying them by numbers instead of names. Victims, witnesses, complainants, and other interviewees should be informed as to whether and how their identities will be protected and whether their names will be recorded and/or used.

 **Step Four: Assess the allegation or incident and conduct further inquiry, if warranted:** After receiving and recording an allegation or incident report, PIU typically assess the seriousness and credibility of the claim against existing security policies and procedures to determine any noncompliance by security personnel and whether further investigation is needed. A more in-depth inquiry should be conducted in cases of serious allegations or incidents, such as instances of unlawful or abusive acts by security personnel, and/or where severe impacts result from a security incident, such as injury, sexual violence, use of lethal force, or fatalities. Behavior that may be considered criminal should be referred to the relevant authorities.

 **Step Five: Document the process:** The allegation or incident and the inquiry process should be documented, including sources of information, evidence, analysis, conclusions, and recommendations. Where it is not possible to reach a conclusion (for example, due to limited or contradictory information or evidence), the efforts being made should be stated clearly along with any efforts to fill gaps and make further assessment. It is good practice for information related to security allegations or incidents to be classified and handled as confidential. Any report should be objective, impartial, and fact-based.

 **Step Six: Report any unlawful act:** Potentially criminal wrong doings or unlawful acts of any security personnel (whether employees, contractors, or public security forces) should be reported to the appropriate authorities (using judgment about reporting in cases where there are legitimate concerns about treatment of persons in custody). PIU is advised to cooperate with criminal investigations and ensure that internal processes and inquiries do not interfere with government-led proceedings.

 **Step Seven: Take corrective action to prevent recurrence:** Action should be taken to ensure that negative impacts are not repeated. This may entail corrective and/or disciplinary action to prevent or avoid recurrence, if the incident was not handled according to instructions. In general, PIU is encouraged to identify lessons learned from the incident and take the opportunity to revise internal company policies and practices as needed.

 **Step Eight: Monitor and communicate outcomes:** Since PIU or contracted organizations (PCO) are controlling their own internal processes, they could help ensuring consideration of any allegation or incident is professional and progresses at a reasonable pace. Additional oversight may be needed with regard to third-party inquiries, such as those undertaken by private security providers. PIU and PCO are encouraged to actively monitor the status of any ongoing criminal investigations led by government authorities.

 It is also be good practice to communicate outcomes to complainants and other relevant parties, keeping in mind confidentiality provisions and the need to protect victims. Where appropriate, it can also be constructive to share relevant lessons learned and any efforts to incorporate these into company policy and/or practice.

### 5.9.2. Procedures to manage risks of sexual harassment from security personnel

Special gender considerations are so important in sexual exploitation and abuse related security risks, as women often have different experiences and interactions with security personnel. For example, the potential for sexual harassment or sexual violence against women can increase from an expanded presence of private or public security forces in a project area. Thus, consulting women separately may offer important perspectives and may help companies identify a fuller range of potential risks and community concerns. At the same time, security personnel’s awareness of and respect for culturally specific gender issues may help the local population accept their presence.

 Before engaging to the security service provision, each of employed or contracted security guards or pubic security personnel deemed to be deployed in project area, shall take GBV related induction training and shall capture some awareness on what constitute a sexual harassment or abuse. Moreover he/she has also must be briefed, understand and sign program’s sexual exploitation and abuse code of conduct, which will be part of the employment contract.

 If gender-based violence or sexual exploitation and abuse allegations are egressed on public or private program security personnel or do issues arise from public report or are alleged during project implementation or supervision, PIU project social safeguard expertise must be alerted immediately. Project gender expertise is also advised to consult the Bank’s Good Practice Note and Project SMP on Recommendations for Addressing Gender-based Violence involving security personnel. Grievances that deal with gender-related allegations must be handled very carefully, with respect for the confidentiality of the complainants, survivors and their families.

### 5.9.3 Measures to Manage OHS Risks to Security Personnel

The following measures are recommended risks to security personnel:

* Speed of vehicles used for security purpose should be controlled in the work area and on public roads, to the extent possible.
* Security vehicles should be operated by competent personnel.
* Flagmen should be assigned to coordinate traffic in the work area.
* Traffic signs should be used in the work area.
* Safety zones must be created in the work area with the speed of the traffic taken into account.
* Ensure that adequate ingress and egress is provided for security personnel in their duty stations and throughout the work area.
* Excavation near security personnel workstations should be provided by edge protection to prevent falling in.
* Security personnel working on watch towers and other activities involving work at height should be provided with safe access ladder/stair and a work area which is fully boarded, fitted with guard rails, toe boards, and outriggers.
* Ear plugs or mufflers should be used by security personnel to reduce high pitch noise as long as it interferes their ability to do their work. Continuous noise and vibration generating works should be limited, to extent possible. Security personnel rotation can be considered to reduce the effect of noise on them. Similar, face masks shall be used for work activities generating dust.
* To the extent possible, security personnel workstations should be away from electricity/energy sources and lines. Where electricity/energy lines are available, there should be sufficient separation distance between the security personnel workstation and the lines. Safety signs should be provided indicating the electrical hazard.
* Housekeeping of the security personnel workstations should be maintained, at all times.
* Ensure that all waste is disposed frequently and properly, away from security personnel workstations. Security personnel should be given face masks, sanitizers, condoms, etc to protect them from transmittable diseases. Awareness creation training should be given to security personnel on prevention of transmittable diseases.
* To the extent possible, security personnel workstations should protect them from weather exposure. Provide sheds at workstations. Rotate security personnel to reduce exposure to the elements.
* Psychological stress on security personnel can be reduced through rotation and limiting the working hours.
* Security personnel who have been a victim or involved in an incident should not be left alone in the period following an incident. Psychological support should be provided, if necessary.
* Security personnel should be sufficiently trained to manage emergency situations including on emergency preparedness and response. Project security personnel should work closely with local, regional, and federal security apparatus to obtain up to date security information so that risks can be avoided or better managed.
* Security personnel should not expose themselves to danger unnecessarily and recklessly.
* Ensure quick means of communication between workers, security personnel, and government security apparatus in case of emergency. Make sure that communication equipment is always in good working conditions.
* Firearms should be kept in good condition and stored in suitable and secure locations.
* Security personnel should be well trained in handling firearms. Firearms should not be handled by other project workers.
* Security personnel should wear protective equipment, particularly those related to their work.
* Keep the number of lone and isolated workers to the minimum to handle emergency situations.
* Mitigation measures included in the project Labor Management Procedures (LMP) should be considered for the general OHS risks to project workers.
* Further reference shall be made to the relevant WBG EHS Guidelines to manage OHS risks to security personnel.

## 5.10. Operational Security

Operational security is the essential human overview and involvement and include designated personnel to oversee; monitoring of risk management, assessment and health and safety protocols; Manned guarding; Entry and exit monitoring; Locking away and security marking of plant, tools and equipment, hazardous materials, etc.; Managing and operating technology which supports security, such as setting alarms and automated systems. For this project should also be training, training on potential hazardous materials on site, proper equipment to report events (telephone, radios, etc.), proper training and equipment to deal with potential events due to incurrences into construction site (e.g., fires, release of hazardous materials).

Further to the above, mitigation measures for OHS risks to security personnel identified in Section 4.5.1 include:

* Speed of vehicles used for security purpose should be controlled in the work area and on public roads, to the extent possible.
* Security vehicles should be operated by competent personnel.
* Flagmen should be assigned to coordinate traffic in the work area.
* Traffic signs should be used in the work area.
* Safety zones must be created in the work area with the speed of the traffic taken into account.
* Ensure that adequate ingress and egress is provided for security personnel in their duty stations and throughout the work area.
* Excavation near security personnel workstations should be provided by edge protection to prevent falling in.
* Security personnel working on watch towers and other activities involving work at height should be provided with safe access ladder/stair and a work area which is fully boarded, fitted with guard rails, toe boards, and outriggers.
* Ear plugs or mufflers should be used by security personnel to reduce high pitch noise as long as it interferes their ability to do their work. Continuous noise and vibration generating works should be limited, to extent possible. Security personnel rotation can be considered to reduce the effect of noise on them. Similar, face masks shall be used for work activities generating dust.
* To the extent possible, security personnel workstations should be away from electricity/energy sources and lines. Where electricity/energy lines are available, there should be sufficient separation distance between the security personnel workstation and the lines. Safety signs should be provided indicating the electrical hazard.
* Housekeeping of the security personnel workstations should be maintained, at all times.
* Ensure that all waste is disposed frequently and properly, away from security personnel workstations. Security personnel should be given face masks, sanitizers, condoms, etc to protect them from transmittable diseases. Awareness creation training should be given to security personnel on prevention of transmittable diseases.
* To the extent possible, security personnel workstations should protect them from weather exposure. Provide sheds at workstations. Rotate security personnel to reduce exposure to the elements.
* Psychological stress on security personnel can be reduced through rotation and limiting the working hours.
* Security personnel who have been a victim or involved in an incident should not be left alone in the period following an incident. Psychological support should be provided, if necessary.
* Security personnel should be sufficiently trained to manage emergency situations including on emergency preparedness and response. Project security personnel should work closely with local, regional, and federal security apparatus to obtain up to date security information so that risks can be avoided or better managed.
* Security personnel should not expose themselves to danger unnecessarily and recklessly.
* Ensure quick means of communication between workers, security personnel, and government security apparatus in case of emergency. Make sure that communication equipment is always in good working conditions.
* Firearms should be kept in good condition and stored in suitable and secure locations.
* Security personnel should be well trained in handling firearms. Firearms should not be handled by other project workers.
* Security personnel should wear protective equipment, particularly those related to their work.
* Keep the number of lone and isolated workers to the minimum to handle emergency situations.
* Mitigation measures included in the project Labor Management Procedures (LMP) should be considered for the general OHS risks to project workers.
* Further reference shall be made to the relevant WBG EHS Guidelines to manage OHS risks to security personnel.

Additional measures are included in Annex 2. More detailed information on OHS mitigation measures is available in a standalone LMP document.

Training needed for construction workers, community workers and security personnel with each category of workers training designed for the type of worker. The contractor and community will arrange a more definitive approach/process including costs and effort involved for more contractual or obligatory mechanism. A training module on EHS risks including safety hazards at project sites and flooding, as well as emergency preparedness and response procedures will be also prepared. All the costs related will be considered as part of the contractual agreement and will be included. Below are General Good Practices that guides in building a construction site security plan. Also, the WBG EHS Guidelines provide further OHS requirements and measures. Additional measures are included in Annex 2.

* Establish a written Security Policy for the site.
* Develop a specific job site security plan.
* Refer the project LMP and WBG EHS Guidelines on OHS requirements and mitigation measures to include in the site security plan.
* Assign supervisory security responsibilities.
* Encourage security awareness among all workers.
* Contact the police and fire departments before starting a job to establish cooperative efforts for site security.
* Establish contact with management of adjoining properties - encourage them to report suspicious activities on the site.
* Require prompt reporting by workers of incidents of theft and vandalism.
* Report all losses to the police immediately.
* Maintain complete records of all security incidents.
* Become involved with local groups or associations working to prevent construction-site theft and vandalism.

 **Safety While on the Site**

* When possible, enclose the job site with a security fence.
* Ensure safe ingress and egress to the site.
* Provide nighttime lighting of the site.
* Provide limited access to the site at all times, preferably with lockable gates.
* Maintain a clear zone adjacent to fencing.
* Post warning signs to help keep unauthorized persons off the site.
* Use only high quality locks – never leave keys in locks or leave locks in an open position.
* Inspect the site at the end of each day before securing it, to assure nothing has been compromised.
* Provide parking areas outside of the site for employees and visitors.
* Consider the use of security guards, and have them patrol the site on designated rounds. Provide all security guards with a means of communication.
* Consider limiting vehicle access to the site to one designated entrance through which all vehicle traffic flows.
* Consider installing a portable CCTV monitoring system to capture vehicle traffic entering and exiting the site.

**Safeguarding your Equipment, Tools and Materials**

* Consider utilizing a secured area within the site for equipment storage (e.g., storage trailers or sheds in secured areas).
* Ensure good housekeeping of equipment storage areas. Develop a program to maintain good housekeeping.
* Maintain an inventory control system for all equipment, tools, and materials. Include photographs of equipment and expensive tools. Establish a program for verifying all deliveries.
* Mark all tools and equipment in a conspicuous, distinctive manner to allow for easy identification.
* Consider registering high value equipment with iron watch or help tech to improve the likelihood of recovery if you are the victim of heavy equipment theft.
* Implement a checkout system for all tools and equipment. Post a sign stating, “ATTENTION! ALL TOOLS MUST BE SIGNED OUT.” Also, in addition to written signs, use pictorial signages to reach people with different levels of literacy.
* Keep tools securely locked in storage trailers or sheds in secured areas.
* Stamp all heavy equipment and attachments with an ID number. Provide warning signs on equipment indicating that ID numbers are recorded.
* Establish a supervisory key control program for motorized equipment.
* Lock all equipment cabs during non-working hours.
* Immobilize equipment by disabling it or using anti-theft/anti-vandalism devices.
* Lock oil and gas tank caps, where possible, as a means of deterring vandalism.
* Park equipment centrally in a well-lit, secure area.
* Provide a secure storage area for target building materials.
* Keep the on-site inventory of materials to a minimum.
* Store equipment, materials, and tools away from perimeter fencing.
* Remove equipment and materials from the site when no longer needed – do not use the site for storage. Carefully supervise all trash removal from the site.

 **Strengthen the coordination with Labor and skill offices**: the project office (PIU) will closely work with different levels of labor and skill offices particularly on activities related to the assessment and implementation, monitoring and evaluation of health and safety protocols.

 **Manned guarding and capacity building**: In all stages of the sub-project implementation (particularly during construction and operation), manned guarding is necessary to protect the public assets and also life in case of schools, health facilities both for human and Animal. This also applies for other kind of sub-project. The project properly recognizes the importance of well-trained security guard. Thus, the project will strongly work with the security guards recruited in each sub projects of all stages of the project implementation to have the required skill and knowledge including how to make inspection in Entry and exit monitoring; communication mechanisms with the nearest security (police and other security office) when additional support is needed. The public security forces are accountable to the constitution of the country for any human right abuse and excess force they use. Implementation of EA-RDIP witnessed that there was no significant use of security personnel, consistent with ESS 4.

* Security focal persons will be assigned at PIU and RPIU before project effectiveness.
* Security provisions for workers involved in the distribution of innovative technologies and different public work inputs.
* Hiring third party monitor(s).

## 5.11. Performance Monitoring and Reporting

 Prepare and submit to the PIU/RPIU regular monitoring reports on the SRM performance of the Project, including but not limited to the implementation of this SRMP; status of preparation and implementation of risk management documents required under the ESCP; stakeholder engagement activities; and functioning of the grievance mechanism(s).

### 5.11.1. Site Visits

###

The Woreda level safeguards focal person along with federal and regional level experts in the PIU and RPIU should plan for and implement site visits to monitor Project security risks and arrangements. The frequency of the site visits may be determined as necessary, but annual visit is the minimum requirement. To track program security performance, site visit will use different modalities of collecting information including:

**Schedule meetings with key personnel:** As part of scheduling meetings and the required Security Briefings, ensure that relevant site management personnel are included to be able to provide and discuss security-related information, including: (a) Woredaproject coordinators, Program/Site Manager, woreda/cluster safeguard focal persons (who has overall responsibility for program risks); (b) Security coordinators, Protection Manager (or person responsible for security); (c) Community Relations Manager; (d) civil societies and private actors and (e) Human Resources Manager, Environment and Safety Manager.

 Request assistance in arranging meetings with external stakeholders, including, as appropriate: (a) Public Security representatives, where possible and appropriate (e.g., local senior police officer, local militia, regional special force military commander, etc.), (b) Local public authorities (head of city administration, city peace and security officers; etc.); (c) Municipal authorities; and (d) Local community members: Seek information on community members’ concerns, where possible. If the topic of security personnel may be raised, it is good practice to not have security personnel present during meetings with community members or civil society, even if this means that a meeting location needs to be switched to a more neutral location; (e) Reiterate the commitment to the Code of Conduct (See Annexes 8 and 9) and grievance mechanisms.

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

 The above means of collecting on-site information for monitoring security management involve asking questions of many different stakeholders. This can help gain new information as well as confirm previously collected information or insights. Site-visit questions during program implementation should aim to assess understanding of the essential elements of the security arrangement prepared for a specific Bank program (e.g. any codes of conduct, training content, protocol of security responses, reporting procedure), what security response has been to past incidents, and issues in implementing the security arrangement/security management plan.

### 5.11.2 Oversight

 MInT/PIU and any Contracted Organization, as part of their oversight responsibilities, should monitor site performance of their security personnel on an ongoing basis to ensure professional and appropriate conduct. This may include reviewing policies and materials, undertaking periodic audits, potentially assisting with or supporting training, and considering any allegations of unlawful or abusive acts by security personnel. Speaking to program employees and local community members who come into regular contact with security staff can also provide valuable insights to monitoring the performance of program security management.

### 5.11.3 Joint Implementation Supervision Mission (JISM)

The SMP should be reviewed during supervision missions by the program implementing entities and the development partners. Depending on the assessment of program security performance, appropriate corrective actions may be proposed. As part of program supervision, the World Bank staff review incident reports submitted to the Bank, and grievance mechanism logs regarding grievances or allegations that involve project-related security personnel.

 Security-related allegations or incidents can include issues such as theft, abuse of power and retaliation, sexual harassment and exploitation, gender-based violence, and bribery and corruption. Bank staff should request more information about any reported incidents and steps taken to address the issue and prevent recurrence and should promptly keep Bank management informed of allegations or instances of violence or abuse and the remedial efforts. Allegations or incidents related to security personnel should be documented and assessed with the objective of determining compliance or noncompliance with policies and procedures and whether any corrective or preventive actions are required.

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

### 5.11.4. Independent Security Audit

The Security management plan should be reviewed during supervision missions by the Bank. Depending on the assessment of the program security performance, an independent security audit may be proposed for basic corrective measures. Besides, significant changes in the program’s security situation should be reported immediately to the Bank. Depending on the nature and severity of security impacts, an independent security audit may be undertaken which will allow for the necessary changes/updates to the SMP or ESCP.

At this initial stage of the program, an independent security audit timeline is suggested to be every six-month period of program operation, which then could be scheduled annually for later stage of program operation. Where incidents or grievances regarding security have been identified, the risk profile of the program may need to be changed, and Bank’s supervision may need to increase, such as more frequent monitoring trips or the use of third-party monitoring.

### 5.11.5. Communicating the Outcome of Complaints

 Project staff responsible for program SEP and Grievance Mechanism should communicate outcomes to complainants and other relevant parties, keeping in mind confidentiality provisions and the need to protect victims from further incidents or retaliation. Where appropriate, it can also be constructive to share relevant lessons learned with the community and any changes made to prevent future incidents.

### 5.12 Managing Public or Government Security Engagement

Public security forces involvement in EA-RDIP site shall only be encouraged on special demanding circumstances and they should not be involved in protecting specific program activities on a regular basis. The involvement of public security shall only be considered only for typically broader-community context level instabilities or fragile security conditions. Because of this, public security forces involvement in EA-RDIP sites could typically be driven by:

 The request of the MInT/PIU, due to a perceived increase in the security threat level, for example, in program areas with instable, fragile and conflict situation; risk of attacks from armed insurgents, instances of road closure by ethnic/border conflicts Ethiopia demand or put as a requirement. Generally, the program related security issues are encouraged to rely first on project-owned or contracted individual security forces to solve site security problems, not think of public security forces as a priority or as a replacement for contracted security forces. But, if this option fails, the GoE or the regional government may require deploying public security.

 Option of working with public security forces can be the most challenging aspect of security management for PIU, as it do not control the decisions of public security personnel or may have limited influence in this regard. For this reason, the engagement of public security in EA-RDIP should take the following key management-considerations. As part of the ESS4, following the risk assessment a suitable mitigation measure is put in place.

### 5.12.1. Signing a Memorandum of Understanding

A memorandum of understanding (MoU) is a formal, written agreement between the PIU and concerned woreda/regional government authorities and commanding unit of the local/regional/federal security forces. The MoU should establish and document agreed key expectations and decision-making processes and procedures with regard the engagement of public security personnel. It allows PIU, local government and public security forces to delineate their respective roles,

 There are many different ways to construct the MoU. In general, it is recommended that: (a) the MoU include references to program SMP, national laws, WB’s ESSs and other applicable international laws such as relevant UN protocols; (b) the MoU typically includes any financial or resourcing issues (such as housing, food, stipends, transportation, and the like); and (c) where possible, it is recommended that PIU includes a provision allowing them to request the removal of individual public security personnel from their area of operations. It will also include a project code of conduct, focusing on human rights and well managed use of force.

### 5.12.2. Communication and engagement with public security

MInT/PIU is advised to communicate their principles of conduct to public security forces and express their desire that the security provided be consistent with those standards. The degree and formality of this communication may vary according to the security risks and the nature (and appropriateness) of the security arrangements involving public security personnel. PIU should keep a record of any communication or communication attempts with public security personnel. It shall also develop or establish a functional activity/incidence reporting mechanism for other relevant stakeholders (see Annexes 3, 4, and 5 for incident reporting templates).

 **Low-risk contexts:** If the number, type, and nature of the deployment appears appropriate and proportional to the assessed risks, PIU may wish, at a minimum, to simply maintain contact and communication through check-ins with public security forces to help the program be confident that police will respond quickly and professionally if an incident occurs, or that suspects (including community members) caught trespassing or stealing will be treated fairly in police custody.

 **High-risk contexts:** In high-risk contexts, having a more formalized and established relationship can be central to ensuring that any potentially tense and dynamic situations do not escalate to become even more volatile due to police or military involvement. The situation can be exacerbated if the risk of excessive force by public security personnel seems high.

 **Proper handover:** When public security is needed to protect program workers and property, there should be a proper handover of control from contracted/privately employed security guards to public security and a way to manage handing the control back when the situation is stabilized. This can be a good topic to start a discussion, because it focuses on public security’s legitimate role and on assuring the greatest effectiveness and safety.

## 5.13. The Estimated cost of risk mitigation and prevention measures for the project

Table18: Security Management Budget

|  |  |  |
| --- | --- | --- |
| **Item** | **Cost-USD** | **Frequency** |
| Project security manager  | 24,000 | Annual |
| Training | 250 | Per person |
| Fire safety equipment | 200 | Per site |
| Guarding Services including guard equipment (if applicable) | 2,000 | Monthly/per site |
| First Aid Kit | 100 | Per site |
| Hibernation Kits | 250 | Per Office/site |
| Physical security measures (e.g. locks, doors, safes, window grills) | 4,000 | Per Office/site |
| Independent security audit | 5,000 | Per field visit |
| Hostile Environment Awareness Training (HEAT) | 5000 | Along the project implementation |
| Other security measures (e.g. fencing, lighting, signages, monitoring system, PPE) | 5,000 | Per site |

Table : Summary of risks and management framework for SRA and SMP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Security Risks Identified*** | ***Proposed Mitigation Measures***  | ***Risk Rating*** | ***Budget Timeframe*** | ***Responsible Body*** |
|  Armed robbery | Enhanced Information and Communication platforms between Woreda program implementation unit and local public security forcesIncreased coordination and information sharing on potential security risks from armed groups operating in the area with other trusted public security actorsThorough risk assessment and contextual analysis, in addition to routine measures (counter-terrorist search, hostile surveillance and reconnaissance detection and convey escort/protection if applicable), necessary for detecting armed groups presence in the areaSuspension of program activities in program areas (located within 25 Km of the incident’s place), presence of armed groups is detected. | Medium | Throughout the project implementation | PIULocal and regional officialsLocal and regional security officialsContracted firmsProgram security focal person |
| Armed conflict between government and non-government forces | Conducting socio-economic conflict analysis to understand the root cause of border conflicts in program implementation areas.Map out’ warring factions, individuals, organizations and strategies that could help resolve border conflictsEarly identification and management of conflict Intensifying factors: ethnic conflict, recent violence, historic animosity, weakness of claimant groups (to control potential break-outsIdentify conflict ‘warning signs’. Communities can make a list of warning signs that would be evidence of increasing border tensions within or between communities | Medium | Throughout the project implementation | PIU at the MInTContracted firmsPublic security PersonnelPrivate security personnelworeda peace and security bureau |
| Theft to construction materials at a project site | Site access control: guidelines for security personnel on how to interact with community members seeking access to Program site or raising a concern (for example, training on the grievance mechanism and Code of Conduct).Use of physical security personnel.premises fencing especially materials areas, storage areas like construction sitesEstablish formal and consistent reporting and communications mechanisms with local police and other security related stakeholders.Strengthen physical security measures (fence, gate check, store lock)Assign additional security guard in collaboration with local administrationAssessment and health and safety protocols. Manned guarding: Entry and exit monitoring; Locking away and security marking of plant, tools and equipment, hazardous materials, etc.Managing and operating technology which supports security, such as setting alarms and automated systems. Training on potential hazardous materials on site, proper equipment to report events (telephone, radios, etc.), Proper training and equipment to deal with potential events due to incurrences into construction site (e.g., fires, release of hazardous materials).  Training needed for construction workers, community workers and security personnel with each training designed for the type of worker. | Medium | Throughout the project implementation | Woreda EA-RDIP program coordinatorprogram Security focal person/coordinatorLocal police |
| GBV/SEA | • Fully implement sanctions contained in the GBV Action Plan (Please refer GBV Action Plan Annex 6 on the ESMF).-Strengthen treatment and referral pathways for GBV/SEA survivors-Raise awareness on GBV/SEA protocols for the Project in line with LMP -Provide separate ablution facilities for men and women at the workplace -Ensure proper lighting on the compoundsFully implement sanctions contained in the GBV Action Plan (Please refer GBV Action Plan Annex 6 on the ESMF). | Medium | Throughout the project implementation | Federal, regional, woreda PIU, and administratorsContractors and sub-contractorsImplementing Agencies,Security players in the devolving government structures |
| Local conflict occurs between ethnic groups and clans | Ensure PIU recruits, equips, and trains security forces consistent with Program SMPConducting socio-economic conflict analysis to understand the root cause of border conflicts in program implementation areas.Map out’ individuals, organizations and strategies that could help resolve border conflictEarly identification and management of conflict Intensifying factors: ethnic conflict, recent violence, historic animosity, weakness of claimant groups | Medium | Throughout the project implementation | PIUPublic Security Officials and Army CommandsLocal Political Officials |
| Labor influx and women trafficking | * Communicate expectations regarding appropriate conduct, together with disciplinary measures;
* Depending on the nature of the project, adoption of a formal code of conduct.
* Prevent any kind of involuntary or compulsory labor, such as indentured labor, bonded labor, or similar labor-contracting arrangements.
* No trafficked persons will be employed in connection with the project.
 | Medium | Throughout the project implementation | Federal, regional, city PIU, and administratorsContractors and sub-contractorsImplementing Agencies,Security players in the devolving government structures |
| Trespassing | * Cultivate strong community relationships and information sources
* Coordination and deconfliction with Ethiopian Defence Forces and regional armed forces
* Ensure pre-departure checks are carried out ahead of all journeys
* Recruit dedicated security coordinator to oversee mitigation measures and incident management
 | Medium | Throughout the project implementation | PIUPublic Security Officials and Army CommandsLocal Political Officials |
| Community protest | * Liaison with all interlocutors at all levels including government security forces, civil society, other parties to the conflict and project beneficiaries
* Ensure minimum physical security measures are in place for Staff accommodation when not residing in a Humanitarian Hubs.
* IDs provided for identification of staff/project personnel
* Where private guards are present, training on active and hostile surveillance and managing crowds
* Evacuation/relocation plan in place for EA-RDIP II staff
 | Medium | Throughout the project implementation | PIUPublic Security Officials and Army CommandsLocal Political Officials |
| Unmet community expectations, or where benefit sharing is perceived to be lacking or unfair | * Strictly adhere to the provisions set in Project Implementation Manual
* Accessible and repeated community members consultations composing both program participant ,non-participant community members and local administration representatives
* Establish and strengthen locally accessible program grievance redressing/ handling mechanism.Designing a program membership arrangement that permits new membership opportunities vis-à-vis with certain commitment requirement
 | Medium | Throughout the project implementation | PIUProgram social safeguard coordinatorsWoreda/local administration n bureau |
| Acts of violence | * Minimize on site cash storage, keeping petty cash amounts.
* Access control procedures in place as per areas SRM.
* Security briefings and training.
* Liaison with interlocutors including government security forces
* Incident reporting process that should include local authorities
* Staff constant advice on maintaining low profile
* Security staff accompanying missions, where deemed necessary by a security risk assessment.
 | Medium | Throughout the project implementation | PIU at the RPIUContracted firmsPublic security PersonnelPrivate security personnelWoreda peace and security bureau |
| Burglary of workplace/residence | * Access control in place at all sites, as far as reasonably practicable
* Use of unarmed guards/ watch people at project sites
* Asset management procedures, including inventories
* Secure storage of assets, such as warehousing, as outlined in the SOPs
* Seek insurance for high value items
* Recruit dedicated security coordinator to oversee mitigation measures and incident management
* Cultivate strong culture of incident reporting and follow-up
 | Medium | Throughout the project implementation | Woreda EA-RDIP II project coordinatorprogram Security focal person/coordinatorLocal police |
| Intimidation and discrimination | * Constant engagement with community leaders in EA-RDIP II operational areas.
* Liaison with interlocutors including government security forces
* Security briefings and adhoc training to raise situational awareness among personnel
* Incident reporting process that should include local authorities
* Staff constant advice on maintaining low profile
* Security staff accompanying missions, where deemed necessary by a security risk assessment.
* Relocation plan in place for EA-RDIP II and MInT staff
 | Medium | Throughout the project implementation | Federal, regional, Woreda PIUContractors and sub-contractorsImplementing Agencies Security players in the devolving government structuresRegional and Woreda Administration |
| Abduction/Kidnapping and hijacking: | * Use of physical security personnel,
* Ensure consistent reporting and communications mechanisms with public security forces and other stakeholders.
* Staff should avoid travel in darkness; only using trusted drivers / ; not set patterns and routines; keep in pairs or teams at all times.
* Local knowledge of the program/subproject area and operational context must be maintained by staff at all times.
* Seek information from project security focal person and clearance from PIU coordinator.
* 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.
* SRAMP should be made available to all staff and appropriate training conducted.
* Never fight back when apprehended with armed people
* Do not try to argue or make provocative comments.
* Do not stare or make eye contact with the kidnappers.
 | Medium | Throughout the project implementation | Federal, regional, woreda PIUContractors and sub-contractorsImplementing Agencies Security players in the devolving government structuresRegional and Woreda Administration |
| Financial corruption | * Staffing reforms promote competition, performance/merit based career structures.
* Disclosure of assets
* Transparent appointment of qualified administrative leaders (and selection of political leaders)
* Ring-fencing finances of utilities, separation of roles between local government and utilities
* Support for improving integrity of business (professional associations, codes of conduct)
* Demonopolizing operations and maintenance
* Financial and technical audits and reporting
* Performance-based contracts with defined minimum standards
* Transparency in operations and management
* Citizen role in oversight
* Benchmarking utility performance Small/informal providers
* Improve interface between formal and informal
* Legitimization
* Formal bulk supply, pricing, competitive tenders for franchises
 | Medium | Throughout the project implementation | City EA-RDIP II project coordinatorprogram Security focal person/coordinatorLocal police |
| OHS risk to the security personnel | -Further reference shall be made to the relevant WBG EHS Guidelines to manage OHS risks to security personnel.-Conduct regular training and awareness project focused on the key and relevant content of international and national guidance, the ESMP, Code of Conduct, accident and incident reporting, accident root cause analysis and remedial measures, projects for project workers, community and IAs;Environmental and Social Clauses for Contractors Consultation (it will be included in bids and contractors’ contracts)Adhere to Hazardous material and Wastes Management set out in the ESMFAdhere to Labor Management Procedures (LMP).Adhere to Liquid and Solid Waste Management Guideline prepared for EARDIP II.Ensure ESHS/OHS provisions are incorporated in the bidding documents and contract agreement for construction.Design and implement a contingency plan/site-specific OHS plan to manage potential accidents or natural disasters in situations of normal operation as well as under state of emergency, based on the vulnerability of the country to natural disasters; the plan must include an Occupational health plan and be approved by the Ministry of Health/MInT ESHS or OHS unit.Train personnel and workforce in the implementation of the contingencyPlan/site-specific OHS plan.Ensure that waste management is operable to reduce the fuel element for fireEnsure a fire alarm/smoke alarm system is operable within the sitesConduct regular Environmental and Social Monitoring and audit (the security monitoring will be included in regular E&S monitoring).Conduct regular emergency drills at project sites in coordination with relevant local authorities.Evaluate potential exposure toworkers against the reference levels developed by the International Commission on Non-Ionizing Radiation Protection (ICNIRP).Take into account security personnel’s perception about Electromagnetic Fields (EMF) by consulting with the local community after the sitingprocess of antenna towers.Limit public access to antennae tower locations.Levels of EMF in workplaceIdentify potential exposure in theworkplace Train workers in the identification of occupational EMF levels and hazards Identification and establishment of safety zones to differentiatebetween work areas and public areasDevelopment and implementation of an EMF safety program, as set out by the WB’s EHS Guidelines for Telecommunications | Medium | Throughout the project implementation | Federal, regional, city PCUContractors and sub-contractorsEPA in the devolving government structuresRegional and City AdministrationLabor offices E and S specialist and Focal persons |
| Risk due to presence of security forces | * Effecting Contractual arrangements with all involved security guards hence provide clear instructions on expected code of conduct.
* Induction training to recruited security personnel, covering topics like, proportionate use of force, what constitutes sexual harassment, GBV, and program’s asset management system
* Documented disclosure of program’s policy on firearm holding, utilization and disciplinary measures for breaches on code of conduct Establish accessible means of receiving and reporting incidents and allegations regarding misconducts by security personnelAdhere to WB Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel as well as other good international practices and standards.
 | Medium | Throughout the project implementation | PIUContacted private security company |
| **Other Common Security Threats-Not Rated by this Assessment** |
| Insecure road transportation including access blockage to some project regions and Woredas | Enhanced Information and Communication platforms between Worreda program implementation unit and local public security forcesIncreased coordination and information sharing on potential security risks from armed groups operating in the area with other trusted public security actorsThorough risk assessment and contextual analysis, in addition to routine measures, necessary for detecting armed groups presence in the areaSuspension of program activities in forest areas, presence of armed clash is detected. |  |  | PIUContracted firmsPublic Security OfficialsArmy CommandsPolitical Officials |
| Workplace injuries/safety risks, including road safety | Strictly apply the program LMP; purchase and supply of PPE materials; enforce the workplace safety features as per the OHS plan.Awareness raising training on work-place safety cultures, including road safetyEstablishment of first-aid corner or mobile first-aid boxesBasic first-Aid training to program workers and Forest management cooperatives members |  |  | PIU, RPIU and Woreda level focal personRegional and Woreda security officeWoreda administrationSecurity management teamContractorsConsultants |
| Risks related to presence of mobile plant and vehicles, risks related to musculoskeletal health and load loading, and risks related for exposure to chemical agents.  | 1. ***Measures related to mobile plants and vehicles risks***
* Access to vehicles would be limited to sealed and stabilized areas, as far as practicable, to reduce dust generation.
* Ensure that all vehicles entering and leaving the site and carrying a load that may generate dust are covered at all times, except during loading and unloading. Any such vehicles shall be covered or enclosed in a manner that will prevent emissions of dust from the vehicle at all times.
* Movement of vehicles, machinery and equipment will be through designated corridors.
1. ***Measures to exposure to chemical agents***
* Maintenance schedules including engine tuning, filter cleaning, etc. for construction equipment and vehicle will be implemented according to manufacturers’ specifications.
* Chemicals shall be stored in a shaded, cool and well-ventilated area (as per chemical storage requirements). This will help ensure that no fumes of gases are seeping into the surrounding air.
* Onsite repair, maintenance, oil change, cleaning, and washing for the plants, equipment, vehicles, concrete truck mixers, etc. is prohibited.
1. ***Measures related to muscloskeletal healt and load loading***

Elimination, substitution, engineering controls, administrative controls and use of personal protectiveA three-tier hierarchy of controls is widely accepted as an intervention strategy for reducing, eliminating, or controlling workplace hazards, including ergonomic hazards. The three tiers are:1. Elimination

Elimination, or physically removing a hazard from a workplace, is the most effective stage of the hierarchy of controls. When hazards are eliminated or removed from a work environment, they no longer have the potential to negatively impact employees. Though it’s conceptualized as the most effective stage, elimination is also typically the most challenging to implement. Doing so can be costly and require major overhauls in preexisting workplace processes.Examples:• Redesign a process to eliminate the use of hazardous equipment or product• Perform tasks at ground level rather than working high above ground• Store goods at lower heights so workers don’t have to climb tall heights and risk fall injuries or fatalitiesb. SunstitutionSubstitution, or replacing a hazardous item or activity with something less hazardous, is the second-most effective stage of safety control. Substitution serves a similar purpose to elimination, as it removes a hazard from the workplace or decreases the potential for the hazard to negatively affect employees. If a workplace process is still in its design or development phase, substitution can be an inexpensive and streamlined method for managing a hazard.Example:• Replace a caustic cleaning agent with a non-toxic alternative• Substitute a solvent-based paint with water-based paint• Use a non-silica abrasive material instead of sandblasting1. Use of engineering controls

It referes to a method of managing OHS hazards, such as incidents, injuries, and illnesses by isolating employees/workers from the hazard(s). Engineering controls, or designing purposeful solutions that physically separate employees from hazards, are the third-most effective stage of safety control. Many organizations favor engineering controls to remove the hazard at the source, rather than after an employee comes into contact with a hazard. It’s important to note that while engineering controls can sometimes be costly to implement, they typically result in lower overall operating costs due to the new safety features.The preferred approach to prevent and control muscloskeltal health and load loading is to design the job to take account of the capabilities and limitations of the workforce using engineering controlsExamples: • Place barriers around fans and other loud machinery• Fence around dangerous high-voltage equipment• Install guardrails at worksites that are high above ground1. Use of administrative controls (changes in work practices and management policies)

Administrative control strategies are policies and practices such as; operating procedures, work duration protocols and workplace signage protocols that reduce muscloskeletal health and load loading risk but they do not eliminate workplace hazards. Although engineering controls are preferred, administrative controls can be helpful as temporary measures until engineering controls can be implemented or when engineering controls are not technically feasible. Examples:• Limit the time a worker is exposed to a hazard• Create written formalized operating procedures• Install signs, labels and alarmse. Use of personal protective equipment (PPE)PPE, physical equipment worn or used by employees while they perform their work, are the fifth- or least-most effective stage of the hierarchy of controls.PPE generally provides a barrier between the worker and hazard source. Respirators, ear plugs, safety goggles, chemical aprons, safety shoes, and hard hats are all examples of PPE. Whether braces, wrist splints, back belts, and similar devices can be regarded as offering personal protection against ergonomic hazards remains an open question. Although these devices may, in some situations, reduce the duration, frequency or intensity of exposure, evidence of their effectiveness in injury reduction is inconclusive. In some instances, these devices may decrease one exposure but increase another because the worker has to “fight” the device to perform the work. Examples:• Eye and face protection (goggles and masks)• Head protection (hard hats)• Foot and leg protection (foundry shoes)• Hand and arm protection (chemical-resistant gloves)• Body protection (hazmat suits)• Hearing protection (earplugs) |  |  | * PIU, RPIU and Woreda level focal person
* Regional and Woreda security office
* Woreda administration
* Security management team
* Contractors
* Consultants
 |
| Delay in procurement and public work and PPE material supply | 1. Assess and use alternatives including local markets

Coordination with government security bodies incase their engagement and support is needed while transporting construction materials from central market place and to construction sites |  |  | PIU, RPIU and Woreda level focal personRegional and Woreda security officeWoreda administrationSecurity management teamContractorsConsultants |
| Security-posed GBV Risks | * Strictly adhere to the provisions set out in the Program GBV Action Plan developed as part of the ESMF.
* Awareness-raising/training for security personnel (both private and public) on GBV.
* Awareness-raising training for women and local community members
* Grievances that deal with gender-related allegations must be handled very carefully, with respect for the confidentiality of the complainants, survivors and their families.
1. working together, referrals and collaboration with Women and social affairs bureau
 |  |  | PIUContracted firmsPublic/government Security officialsWoreda Women and Social Affairs bureau |
| Incident to project staff and project workers including physical beating and sexual harassment and GBV | -Awareness creation on GBV and social harassment for communities 1. -Limit frequency of field travel to security risk areas
2. -Access updated information on security issues before any movement in to security risk areas
3. -Induct security personnel on the project’s CoC
4. -Ensure contracted security personnel sign the CoC
5. -Strengthen treatment and referral pathways for GBV/SEA survivors
6. -Raise awareness on GBV/SEA protocols for the Project in line with LMP and the ESF
7. -Provide separate facilities for men and women at the workplace
8. -Ensure proper lighting on work sites
9. -Fully implement measures and sanctions contained in the GBV/SEA/SH AP.
10. -Report to and get preventive support from higher security officers (police and regional special force)
* Adherence to requirements of the SEP, GBV/SEA/SH AP, LMP, GRM
 |  |  | PIU, RPIU and Woreda level focal personRegional and Woreda security officeWoreda administrationSecurity management teamContractorsConsultants |
| Impacts from deployment of public or private security personnel | * Effecting Contractual arrangements with all involved security guards hence provide clear instructions on expected code of conduct.
* Induction training to recruited security personnel, covering topics like, proportionate use of force, what constitutes sexual harassment, GBV, and program’s asset management system
* Documented disclosure of program’s policy on firearm holding, utilization and disciplinary measures for breaches on code of conduct Establish accessible means of receiving and reporting incidents and allegations regarding misconducts by security personnel
 |  |  | PIUContracted private security company |

# Annex 1: Escalation Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **EA-RDIP State Alert****Level** | **Alert State GREEN** | **Alert State GREY** | **Alert State WHITE** | **Alert State YELLOW** | **Alert State RED** |
| **EA-RDIP Descriptor**  | Precautionary  | Restriction of Movement  | Stabilization Evacuation | Concentration | Relocation/Evacuation  |
| **Potential****Triggers** | -Agreement by project coordination units at all level and with stakeholders;- Agreement between project implementers and project workers; | - Community unrest/conflict;-Limitation of transportation access to project site-- Limitation of access to targetSites due to insecurity;- Government offices affected in undertaking their day to day activities | - All Grey Status Triggers, andadditionally:- Specific threats against EA-RDIP II workers;- Armed robbery at EA-RDIP II office/ activity location;- Serious injury/illness of project personnel. | - All White Status Triggers,and additionally:- Armed conflict nearby impacting project activities. | - All Yellow Status Triggers, and additionally:- Serious assault/fatality of project workers;- Withdrawal of WB Supported projects from the area (or nearby) location;- Withdrawal/lack of government support to ensure security. |
| **EA-RDIP Response** | - Normal day to day government operations ongoing-Project activity ongoing -Project coordinators and security focal personnel monitor the security situation.  | -undertake site specific security risk assessment- The public security officials to notify project coordinators who will in turn notify project workers within 24 hours. - Government security officers accompany project workers, contractors and suppliers during movement to project site -Temporary suspension of activities; | - Project workers pause field visit to move to safe location;-Project coordinators and security focal personnel to account for workers and project resources regularly.- The public security officials to notify project coordinators who will in turn notify project workers within 24 hours.- Public security officials in liaison with the PIU assess potential for de-escalation.- Update WBG on proposed options for de-escalation for agreement- Implement agreed de-escalation actions - Temporary suspension of activities; | - Project workers to move to concentration points and prepare to relocate to safe location;- Project coordinators and security focal personnel to account for workers and project resources regularly -- The public security officials to notify project coordinators who will in turn notify project workers within 24 hours.- Update WBG on proposed options for de-escalation for agreement- Implement agreed de-escalation actions- Suspension of project activities | - The public security officials to notify project coordinators who will in turn notify project workers within 24 hours - EA-RDIP to review viability of continuing with project activities in a particular location/region- EA-RDIP to advise and agree with WBG on proposed way forward(pause/continue/otherwise)- Suspension of project activitiesyyy |

#  Annex 2- Security Operating Procedures (SOP)

Security Operating Procedures describes key procedures and how these fit together. These are common procedures including boundary security (perimeter and access control), access-point operations (screening of people and vehicles), incident response (who will respond, and how), security patrols, travel security, materials storage and control, information and communication.

The following major operating security procedures should be implemented and put in place to ensure security within the proposed EA-RDIP II subproject sites:

**Boundary Security:** The boundary security in project camps and associated facilities shall be marked by security fences.

**Access-Point Operations:** project staff and visitors will access camps through designated gates. Searches will only be conducted by security personnel who have received instruction and information regarding the procedure and the legal aspects of search and seizure. Body searches will only be conducted by security personnel of the same gender. Above all, implementing agencies, contractors and sub-contractors shall have booking in and out procedure for all regular project workers and visitors.

**Vehicle Access Control Procedures:** All Vehicles accessing project facilities will be accessed through the approaching ways suggested in consultation with community and at the gate with the driver only after going through a security check/search for prohibited items i.e., Alcohol Beverages, Firearms, Knives and dangerous drugs. The driver must declare his entire luggage at the main gate (Personal luggage) for checking. Besides, a vehicle access log will be maintained.

**Vehicles:** All EA-RDIP cars in use for operations to be parked within secured compound. Besides, all vehicles must be licensed and checked periodically, and each vehicle must be equipped with a spare tire, a toolbox, first aid Kit and vehicle logbook. Above all, drivers must abide by the traffic laws and not exceed the speed limit; they must immediately report any traffic accident.

**Prohibited Items:** bringing items such as; knives, guns, alcohol beverages, dangerous drugs, explosives of any type to project sites by workers and visitors are strictly prohibited. The security personnel shall carry out body check and report to the contractor and to the EA-RDIP II-PIU.

**Incident Response:** Any security incidence related to the subprojects directly affecting project staff, equipment and communities should be reported by either the project manager or security personnel in charge to the nearest police post. In the event of a serious insecurity occurrence, the project manager shall report to the EA-RDIP -PIU. The EA-RDIP -PIU will notify the WB Bank within 24 hours.

**Security Patrols:** Security patrols shall be carried out by the security personnel. Where subprojects are located in areas with high potential insecurity incidence, public security services should be used.

**Travel Security:** Travel security will be required where subproject staff and equipment are transiting through areas with security risks. In this case, the arrangement for travel security shall be coordinated by EA-RDIP -PIU or regional implementing agencies in coordination with national information network security agency or regional/local security offices. Travel to high-risk areas is subject to a security risk assessment and that the authority be sought from the PIU Coordinator. Where GSM coverage is not guaranteed, staff should be issued with a satellite phone. Staff should also carry a grab bag, containing food, water, first aid kit, medicines, etc.

**Hierarchy of hazard management**

a. **Eliminate the Hazard:** Determine if the process, plant, equipment, testing methods, materials or substances are necessary.

b. **Substitute the Hazard:** Reduce the risk by substituting a less hazardous process, plant, equipment, testing method, material or substance (e.g. Replace ladder with scissor lift, Substitute solvent based paint with water based paint ,Redesign plant to reduce noise levels, Replace frequent telephone use with headsets).

c. **Isolate the Hazard:** Isolate the hazard by using containment, shielding or distance (Put protection around noisy equipment and Guards over moving parts).

d. **Engineering Controls:** Install barriers, guards, ventilation or alarms to reduce the exposure to the hazard, minimize the size or volume of the hazard. Rearrange the work area and workflow (e.g. Use mechanical aids to reduce manual handling).

e. **Administrative Controls:** Reduce the duration of exposure to the hazard Intersperse high demand or intense activity with lighter, less intense tasks. Establish safe work practices, provide training and supervision appropriate to the level of expertise of the personnel involved. Introduce procedures, signs, permits to increase awareness of the hazard or limit exposure to the hazard. Administrative controls may be used as a secondary measure to supplement the other agreed risk controls (e.g. Job rotation, work instructions, restricting access to the area, keeping the area free of disorder, being prepared for emergencies, and Training and induction projects).

f. **Personal Protective Equipment:** Provide personal protection. This is the last resort because it is the least reliable and requires high levels of supervision, skills and attention. Personal protection may be used as a secondary measure to supplement the other agreed risk controls (e.g. Hearing protective devices, respirators, hard hats etc.)

**Fire:** Flammable and explosive materials should also be managed to avoid uncontrolled reactions or conditions resulting in fire or explosion. Hence, Store incompatible materials in separate areas, and with containment facilities separating material storage areas· Besides, material-specific storage for extremely hazardous or reactive materials should be provide· In addition, select materials of construction compatible with products stored for all parts of storage and delivery systems, and avoid reuse of tanks for different products without checking material compatibility· Furthermore, store hazardous materials in an area of the facility separated from the main production works. In cases, proximity is unavoidable, physical separation should be provided using structures designed to prevent fire, explosion, spill, and other emergency situations from affecting facility operations · Prohibition of all sources of ignition from areas near flammable storage tanks.

**OHS:** EA-RDIP II PIU, IA, Contractors will ensure a safe and healthy working environment recognizing the potential OHS risks related to the project. Accordingly, they will ensure that reasonable precautions are taken to protect workers potentially exposed to project related occupation risks. Hence, IAs, contractors and subcontractors shall assess the risks of injury to workers and local community generated by the activities of EA-RDIP II; providing hostile environment training; provide adequate protective equipment (PPE),

**Preparedness to flooding:**

1. Monitor your surroundings and monitor Weather Radio, local television and radio stations.
2. If a flash flood warning is issued for your area evacuate to high ground/place immediately.
3. Flash floods develop quickly. Do not wait until you see rising water.
4. Get out of low areas subject to flooding.
5. If driving, do not drive through flooded roadways!
6. Assemble disaster supplies: such as drinking water, food, cash, medication and first aid supplies. Battery-powered radio, flashlights, extra batteries.
7. Important documents: medical records, bank account numbers.
8. Be prepared to evacuate: identify places to go, identify alternative travel routes that are not prone to flooding, fill your car’s gas tank and if told to leave, do so quickly.
9. Protect your property: Move hazardous, disconnect electrical appliances and do not touch them if you are wet or standing in water.

**Security Supervision and Control:** Security supervision and control may be undertaken at various levels which may include at the national, regional, subproject sites and at the contractor levels.

The EA-RDIP \_PIU and regional implementing agencies will also work closely with national and regional security offices and other relevant stakeholders to ensure proper management of project security issues which will include:

1. Undertaking security risk assessments and recommend mitigation measures at subproject level;
2. Ensure that security mitigation measures are included in sub-project ESMPs;
3. Monitor potential security risks on subproject sites together with project beneficiaries;
4. With social safeguard specialists, provide training to mitigate social risks of project workers and equipment including security risks;
5. Ensure that the GRM for the project workers is established and implemented and that project workers are informed about it;
6. Monitor the implementation of the workers’ CoC for contracted security personnel.

**Security Training**

To fulfill security related responsibilities project workers, security personnel, community, contractors and other stakeholders at all levels need proper training. This is due to the fact that providing security training and awareness creation is one of the most cost-effective ways of to reduce security threats. The security trainings provided include EA-RDIP II security Risk Assessment and Management plan, health and safety, Security Operating Procedure, incident reporting and response, human rights, GBV/SEA (Please refer GBV Action Plan), Environmental, Social, Health and Safety (ESHS) provisions, EHS risks on safety hazards at the project sites, Stakeholder Engagement Plan, Grievance Redressing Mechanisms, use of force, etc. Moreover, for staff who will be deployed to high risk areas will receive Hostile Environment Awareness Training (HEAT). The Training will be provided by the PIU, contractors and relevant security structures of the government. If the PIU have not the required capacity to deliver fit-for-purpose training, it can outsource the service to the external but capable firm.

**Information sharing and communication**

Regarding the responsibility related to security information sharing and communication focal person assigned at federal, regional and woreda level are responsible. In this regard, communication or information sharing could be Federal, regional and then to woreda or the other way round. For instance, in circumstances where the EA-RDIP -PIU agree with higher level the information sharing and communication will be done by the federal to the regional PIU and the Regional PIU will share to woreda. In cases, where the incident or information are happened at the sub-project level it is starts at the contractor to woreda PIU, the woreda to region, the regional PIU to federal PIU, and the federal PIU shares or communicates to the World Bank. The communication approach would be as set out on the Stakeholder Engagement Plan (SEP) and could be mobile phone, lined phone, email, official letter, fax etc.

# Annex 3: EA-RDIP II related incident and accident reporting procedure

Purpose

The purpose of this procedure is to outline the requirements, methods and outcomes of reporting all incidents and accidents.

1. **Scope**

The following incidents and accidents will be reported, irrespective of the nature and level of severity:

* 1. Fatality and critical injury/illness, illness or injury for which an employee receives/seeks medical attention
	2. First aid treatment, occupational disease,
	3. Property damage and fire
	4. Environmental release (chemical spillages)
	5. Explosions
	6. Exposures to biological, chemical or physical agents and other related.

**3. Roles and Responsibilities**

i) Regional Environmental and Social Safeguard Specialists and Project Coordinators

1. Environmental and Social Safeguard Specialists shall continue and regular monitoring and follow up project related incidents and accidents.
2. Report any project related incidents and accidents within 48 hours to Federal Project Implementing Unit (FPIU).
3. Ensure all woredas are provided with incident and accident reporting Template, and the templates completed.
4. Ensure injured or ill employees have received the required medical treatment and regularly update their health status to the FPIU.

ii) Woreda Environmental and Social Safeguard Focal Persons

1. Shall conduct continuous and regular monitoring and follow up project related incidents and accidents.
2. Report the case to the appropriate local administration entities and other relevant bodies.
3. Ensure the injured persons have received the required medical treatment.
4. Ensure Incident/accident Templates are completed.
5. Report the incident/accident within 24 hours to Regional Project Implementing Unit.

**4. Communication**

This procedure shall be communicated to all project PIUs, contractors and sub-contractors and all relevant bodies.

**5. Evaluation**

Compliance with the accident /incident reporting procedures are monitored regularly as part of Environmental and Social Safeguard Specialists, Environmental and Social Safeguard Focal persons.

# Annex 4: Security incident registration form for sub projects of EA-RDIP II

**Region-----------------------Woreda---------------------- Project name ---------------------**

|  |
| --- |
| Date  |
| **Section 1: recorder /investigator**  |
| Name | Position  |
| **Section 2: Incident description**  |
| Date and time of incident:  |
| Location of incident:  |
| Detail description of the incident: |
| Detail description of the incident from eye wittiness: |
| **Section C: identify the root cause: what caused the incident to happen?** |
| **Section D: Action taken to mitigate or incidents:** |
| **Section E: Recommended corrective action to prevent future:** |

# Annex 5: Occupational Health and Safety incident registration form for sub projects of EA-RDIP II

**Region-----------------------Woreda---------------------- Project name ---------------------**

|  |
| --- |
| Date  |
| Section 1: recorder /investigator  |
| Name | Position  |
| Section 2: Incident description /injury information  |
| Name of injured employee | Age  | Sex |
| Employee`s job title  |
| Date and time of incident: |
| Location of incident:  |
| Detail description of the incident: |
| Detail description of the incident from eye wittiness: |
| Section C: identify the root cause: what caused the incident to happen? |
|  Safety procedures were not followed---------------------Machine failed or safety equipment failed ----------------Lack of proper training (use of the PPE or the machine or other equipment for work) -----------Other, specify………………………… |
| Recommended corrective action to prevent future incidents |
| Corrective Action Taken/Root cause addressed  |

# Annex 6: Steps to conduct Root Cause Analyses (RCA) for a Workplace Accident

1. Conduct root-cause analysis of the incident and identify the sequence of events and factual circumstances. The analysis should identify
2. what failing(s) led to the accident/incident
3. what safety measures were in place, and
4. the risk information/training provided to workers on site/communities.
5. The level of monitoring /supervision of unskilled labor should also be assessed.
6. Recommend actions to be taken to rectify the failure(s) that led to the incident.
7. Review the safety procedures at different sites and identify the health and safety measures to be taken to minimize the risks of future accidents both to workers and to local residents. Site visits should be carried out to a representative sample of construction sites, activities, regions and Contractors as applicable. Health and safety representatives of the Contractors and implementing agencies, as well as other technical counterparts as necessary should be interviewed to gain a comprehensive understanding about health and safety management.
8. Review the OHS measures in Safeguards instruments and plans in construction contracts and recommend enhancements as needed. The assessment should identify what the existing procedures for safe performance of construction activities (excavation,

scaffolding, working at heights, welding, etc.) are and should recommend appropriate procedures should the existing ones have gaps.

1. Review the capacity of Contractors and supervision consultants to implement OHS standards. The assessment should review the training plans for skilled and unskilled labor for effectiveness and propose improvements to the training and communication project so that workers are adequately guided to safely perform their work.
2. Review the existing arrangements for recruiting labor and what type of insurance (life or injuries and occupational health risks) and compensations are provided.
3. Review compliance to the Labor Law and other international treaties by Contractors or Subcontractors.
4. Assess the sufficiency of the measures that the Contractors take to minimize risk on the local communities and communicate with them. Recommend improvements as necessary.

# Annex 7: Content of a Safeguards/Standards Corrective Action Plan (SCAP) Outline

The contents of the SCAP are driven by the findings of the RCA, and are specific to the type of incident, its location, severity, and project implementing capacity to implement corrective and preventative measures. The SCAP will be implemented by the EA-RDIP project implementing unit in the developing government structure for serious and severe incidents, with Bank supervision and support. As a general guide, the SCAP could contain the sections set out in the table below:

| **SCAP Sections**  | **Documentation** | **Possible Actions** | **Timeframe for action closures** | **Monitoring indicators**  | **Responsible body** |
| --- | --- | --- | --- | --- | --- |
| Immediate to near term actions  | Documentation, monitoring and reporting  | Stop works, secure the site, provide medical care and counseling, pay compensation, remediate contamination, notify relevant authorities, design and implement response mechanism, etc.  | Within 3 months  | -No of sites/ subprojects stop work-No of workers received medical care and counseling, received compensation- -No of cases notified to relevant authorities etc. | - Woreda, regional and Federal PIU |
| Medium term/ongoing actions  | Documentation, monitoring and reporting  | Stream-line, consolidate and review existing ESHS/OHS monitoring and reporting tools, with a focus on increased monitoring of leading indicators to increase effectiveness.  | 3-6 months | - ESHS/OHS monitoring and reporting tools stream-lined, consolidated and reviewed  | - Woreda, regional and Federal PIU |
| Contractual agreements /enforcement  | Review bidding/contractual arrangements to determine if existing language is adequate to ensure sufficient onsite presence of qualified and independent safeguards professionals for adequate implementation of the heath safety plan and identify if any adjustments may be necessary for future agreements.  | 3-6 months | -No of bidding / contractual documents reviewed | - Woreda, regional and Federal PIU |
| Medium term/ongoing actions | Risk assessment, processes, procedures and training plans for managing risks  | **example:** update risk assessment and management plans to address: • the chance find, clarifying (i) risk factors such as the geophysical characteristics of excavation areas and depth of excavation, the civil war history, (ii) the detailed written information and maps to be obtained from implementer(s) about past surveys and clearance operations before construction can begin, (iii) situations where mechanical excavation should be chosen over manual excavation, (iv) how to safely conduct manual excavation where mechanical excavation is not possible (with input from the implementer(s) and/or other demining experts), (v) develop an adequate training project for workers. • Fire risk and adequate fire extinguishers placement • Electric risk should also be reviewed, and safe work procedures developed for handling, maintaining and checking electric equipment and extension cords.  | 3-6 months | **-**Updated Risk assessment and management plan | -EA-RDIP Woreda, regional and Federal PMU |
| Medium term/ongoing actions | Permit to work procedure | • Permit to work procedures should be developed for high-risk activities with daily verification and sign-off of competent health and safety officers or supervisors.  | 3-6 months | - No of high risk activities for which work permit procedure developed  | - Woreda, regional and Federal PIU |
| Delayed resettlement compensation | **Delayed Resettlement Compensation example:** update risk assessment and management plans to address: • Based on the RCA determination of the reasons for the continued delays in payment of compensation, put in place an effective strategy for addressing them as necessary • Ensure that all outstanding and new claims are appropriately addressed • Determine whether there were impacts that have not previously been considered (livelihoods/loss of business income, vulnerable groups) for which compensation or assistance may be required • Ensure continuing consultation with Project-affected people and a well-functioning grievance mechanism (GRM) • Monitor implementation and provide fortnightly progress reports • Recruit a separate expert to conduct an audit | 3-6 months | - Updated Resettlement/compensation plan - Resettlement audit conducted - No of PAPs for which delayed compensation addressed  | - Woreda, regional and Federal PIU-Woreda administration |
| Medium term/ongoing actions | Competencies, roles and responsibilities:  | Onsite staffing resources and organizational arrangements dedicated to environment, social safeguards, health and safety by the implementer(s) (e.g., construction company and the supervision consultant) should be reviewed considering the updated risk assessment and findings. This may include adjustments in terms of number, competence, onsite presence, organization, communication and reporting, so that project activities may comply with the EHSH/OHS plan requirements.  | 3-6 months | -No of subproject for which onsite/subproject dedicated ESHS specialist by contractor | - Woreda, regional and Federal PIU-Contractor and sub-contractors |
| High level monitoring and evaluation:  | Once the monitoring and reporting system is consolidated, the supervision consultant and PIU should be able to monitor leading indicators such as near-misses (e.g., a heavy load that falls near a worker), and deviations with high-risk potential (e.g., absence of protective barriers, uninsured workers) based on daily observations by the Contractor and the supervision consultant.  | 3-6 months | -Heavy load that falls near a worker) observed or registered during monitoring,-Deviations with high-risk potential (e.g., absence of protective barriers, uninsured workers) observed, registered or reported during monitoring etc. | -Woreda, regional and Federal PIU |

# Annex 8: Code of Conduct for Contractors’

Code of Conduct (CoC) defines the mandatory Dos and Don’ts expected from each staff member, workers and contractors associated with the project .To build a system for SEA/SH risk prevention and mitigation, the project must:

1. Have all employees of contractors (including sub-contractors) in the project area sign CoCs;

2. Have an effective SEA/SH Prevention and Response Action Plan so that workers understand behaviour expectations and policies, as well as an effective GM. This Action Plan should include training and communication. It should also include plans to make the project-affected community aware of the CoC the project staff have just signed; and

3. As part of the SEA/SH Prevention and Response Action Plan, define accountability and response protocols, which set out the procedures followed for holding individuals accountable and penalizing staff that have violated SEA/SH policies.

**Codes of Conduct from Standard Procurement Document**

 **Code of Conduct for Contractor’s Personnel (ES) Form**

**Note to the Employer:**

The following minimum requirements shall not be modified. The Employer may add additional requirements to address identified issues, informed by relevant environmental and social assessment.

The types of issues identified could include risks associated with: labor influx, spread of communicable diseases, Sexual Exploitation and Sexual Abuse (SEA) etc.

Delete this Box prior to issuance of the bidding documents

**Note to the Bidder:**

The minimum content of the Code of Conduct form as set out by the Employer shall not be substantially modified. However, the Bidder may add requirements as appropriate, including to take into account Contract-specific issues/risks.

**Code of Conduct for Contractor’s Personnel**

We are the Contractor, [enter name of Contractor]. We have signed a contract with [enter name of Employer] for [enter description of the Works]. These Works will be carried out at [enter the Site and other locations where the Works will be carried out].Our contract requires us to implement measures to address environmental and social risks related to the Works, including the risks of sexual exploitation and abuse and gender-based violence.

This Code of Conduct is part of our measures to deal with environmental and social risks related to the works. It applies to all our staff, labourers and other employees at the works site or other places where the works are being carried out. It also applies to the personnel of each subcontractor and any other personnel assisting us in the execution of the works. All such persons are referred to as “Contracture’s Personnel” and are subject to this Code of Conduct.

This Code of Conduct identifies the behavior that we require from all Contractors’ Personnel. Our workplace is an environment where unsafe, offensive, abusive or violent behavior will not be tolerated and where all persons should feel comfortable raising issues or concerns without fear of retaliation.

**REQUIRED CONDUCT**

**Contractor’s Personnel shall:**

1. Carry out his/her duties competently and diligently;

2. Comply with this Code of Conduct and all applicable laws, regulations and other requirements, including requirements to protect the health, safety and well-being of other Contractor’s Personnel and any other person;

3. Maintain a safe working environment including by:

a) Ensuring that workplaces, machinery, equipment and processes under each person’s control are safe and without risk to health;

b) Wearing required personal protective equipment;

c) Using appropriate measures relating to chemical, physical and biological substances and agents; and following applicable emergency operating procedures.

4. Report work situations that he/she believes are not safe or healthy and remove himself/herself from a work situation which he/she reasonably believes presents an imminent and serious danger to his/her life or health;

5. Treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers or children;

6. Not engage in any form of sexual 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;

7. Not engage in Sexual Exploitation, which means any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. In Bank- financed projects/operations, sexual exploitation occurs when access to or benefit from Bank- financed Goods, Works, Consulting or Non-consulting services is used to extract sexual gain;

8. Not engage in Rape, which means physically forced or otherwise coerced penetration—even if slight—of the vagina, anus or mouth with a penis or other body part. It also includes penetration of the vagina or anus with an object. Rape includes marital rape and anal rape/sodomy. The attempt to do so is known as attempted rape. Rape of a person by two or more perpetrators is known as gang rape;

9. Not engage in Sexual Assault, which means any form of non-consensual sexual contact that does not result in or include penetration. Examples include: attempted rape, as well as unwanted kissing, fondling, or touching of genitalia and buttocks not engage in any form of sexual activity with individuals under the age of 18, except in case of pre-existing marriage;

10. Complete relevant training courses that will be provided related to the environmental and social aspects of the Contract, including on health and safety matters, and Sexual Exploitation, and Sexual Abuse (SEA);

11. Report violations of this Code of Conduct; and

12. Not retaliate against any person who reports violations of this Code of Conduct, whether to us or the Employer, or who makes use of the [Project Grievance [Redress Mechanism].

 **RAISING CONCERNS**

If any person observes behavior that he/she believes may represent a violation of this Code of Conduct, or that otherwise concerns him/her,he/she should raise the issue promptly. This can be done in either of the following ways:

1. Contact [enter name of the Contractor’s Social Expert with relevant experience in handling gender- based violence, or if such person is not required under the Contract, another individualdesignatedby the Contractor to handle these matters] in writing at this address [ ] or by telephone at [ ] or in person at [ ];or

2. Call [ ] to reach the Contractor’s hotline (if any) and leave a message.

The person’s identity will be kept confidential, unless reporting of all allegations is mandated by the country law. Anonymous complaints or allegations may also be submitted and will be given all due and appropriate consideration. We take seriously all reports of possible misconduct and will investigate and take appropriate action. We will provide warm referrals to service providers that may help support the person who experienced the alleged incident, as appropriate.

There will be no retaliation against any person who raises a concern in good faith about any behavior prohibited by this Code of Conduct. Such retaliation would be a violation of this Code of Conduct.

**CONSEQUENCES OF VIOLATING THE CODE OF CONDUCT**

Any violation of this Code of Conduct by Contractor’s Personnel may result in serious consequences, up to and including termination and possible referral to legal authorities.

**FOR CONTRACTOR’S PERSONNEL:**

I have received a copy of this Code of Conduct written in a language that I comprehend. I understand that if I have any questions about this Code of Conduct, I can contact [enter name of Contractor’s contact person with relevant experience in handling gender-based violence] requesting an explanation.

Name of Contractor’s Personnel: [insert name]

Signature:

Date: (day month year):

Counter signature of authorized representative of the Contractor:

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: (day month year): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Annex 9: Code of conduct of security personnel

**General Conduct**

1. The PIU, IA or contractor will require their security personnel to, treat all persons humanely and with respect for their dignity and privacy and will report any breach of this Code.

**Rules for the Use of Force**

1. The PIU, IA or contractor will adopt Rules for the Use of Force 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.

**Use of Force**

1. The PIU, IA or contractor will require their security personnel to take all reasonable steps to avoid the use of force. If force is used, it shall be in a manner consistent with applicable law. In no case shall the use of force exceed what is strictly necessary and should be proportionate to the threat and appropriate to the situation.
2. The PIU, IA or contractor will require that their security personnel not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life.
3. To the extent that security personnel are formally authorized to assist in the exercise of a state's law enforcement authority, The PIU, IA or contractor will require that their use of force or weapons will comply with all national and international obligations applicable to regular law enforcement officials of that state and, as a minimum, with the standards expressed in the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990).

**Detention**

1. The PIU, IA or contractor will only, and will require their 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. Member and Affiliate Companies will, and will require that their Personnel, 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.

**Apprehending Persons**

1. The PIU, IA or contractor will, and will require their security personnel to, not take or hold any persons except when apprehending persons to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity. Any such apprehension must be consistent with applicable national or international law and be reported to the Client without delay. The PIU, IA or contractor will, and will require that their Personnel 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.

**Prohibition of Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment**

1. The PIU, IA or contractor will not, and will require that their security personnel not, engage in torture or other cruel, inhuman or degrading treatment or punishment. For the avoidance of doubt, torture and other cruel, inhuman or degrading treatment or punishment, as referred to here, includes conduct by a private entity which would constitute torture or other cruel, inhuman or degrading treatment or punishment if committed by a public official.
2. Contractual obligations, superior orders or exceptional circumstances such as an armed conflict or an imminent armed conflict, a threat to national or international security, internal political instability, or any other public emergency, can never be a justification for engaging in torture or other cruel, inhuman or degrading treatment or punishment.
3. The PIU, IA or contractor will, and will require that their Personnel, report any acts of torture or other cruel, inhuman or degrading treatment or punishment, known to them, or of which they have reasonable suspicion. Such reports will be made to the Client and one or more of the following: the competent authorities in the country where the acts took place, the country of nationality of the victim, or the country of nationality of the perpetrator.

**Sexual Exploitation and Abuse or Gender-Based Violence**

1. The PIU, IA or contractor will not benefit from, nor allow their security personnel 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. The PIU, IA or contractor will, and will require their security personnel to, remain vigilant for all instances of sexual or gender-based violence and, where discovered, report such instances to competent authorities.

**Human Trafficking**

1. The PIU, IA or contractor will not, and will require their security personnel not to, engage in trafficking in persons. The PIU, IA or contractor will, and will require their personnel to, remain vigilant for all instances of trafficking in persons and, where discovered, report such instances to Competent Authorities. For the purposes of this Code, human trafficking is the recruitment, harbouring, transportation, provision, or obtaining of a person for (1) a commercial sex act induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or (2) labour or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, debt bondage, or slavery.

**Prohibition of Slavery and Forced Labour**

1. The PIU, IA or contractor will not use slavery, forced or compulsory labour, or be complicit in any other entity’s use of such labour.

**Prohibition on the Worst Forms of Child Labour**

1. The PIU, IA or contractor will respect the rights of children (anyone under the age of 18) to be protected from the worst forms of child labour, including: a) all forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom and forced or compulsory labour, including forced or compulsory recruitment of children for use in provision of armed services; b) the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances; c) the use, procuring or offering of a child for illicit activities, in particular for the production and trafficking of drugs; d) work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children. Member and Affiliate Companies will, and will require their Personnel to, report any instances of the activities referenced above that they know of, or have reasonable suspicion of, to Competent Authorities.

**Discrimination**

1. The PIU, IA or contractor will not, and will require that their Personnel do not, discriminate on grounds of race, colour, sex, religion, social origin, social status, indigenous status, disability, or sexual orientation when hiring Personnel and will select Personnel on the basis of the inherent requirements of the contract.

**Identification and Registering**

1. The PIU, IA or contractor , to the extent consistent with reasonable security requirements and the safety of civilians, their Personnel and Clients, will: a) require all Personnel to be individually identifiable whenever they are carrying out activities in discharge of their contractual responsibilities; b) ensure that their vehicles are registered and licensed with the relevant national authorities whenever they are carrying out activities in discharge of their contractual responsibilities; and c) will ensure that all hazardous materials are registered and licensed with the relevant national authorities.

# Annex 10: List of SRAMP Study Participants

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Name** | **MDAs** | **Position** | **Cellphone No.** | **email** |
| **Federal Level**  |
| **1** | Yodahe Zemichael | National ID Program Office | Executive |  | yodahe@id.et |
| **2** | Betelihem Mergia | National ID Program Office | M&E Director | 0913555557 | betlhem@id.et |
| **3** | Rahel Abraham | National ID Program Office | Program Director | 0951109771 | rahel@id.et |
| **4** | Sileshi Tadesse | MoWSA-Women Rights Protection | Executive | 0911882233 | Seleshi\_tadesse@yahoo.com |
| **5** | Tefera Fekadu | Development Bank of Ethiopia-DBE | Acting for External Fund, credit and Grant Finance | 0912048040 |  |
| **6** | Gizaw | Development Bank of Ethiopia-DBE | Senior Electrical Energy Expert | 0913338193 | Giz2005@gmail.com |
| **7** | Fetsum Haile | Development Bank of Ethiopia-DBE | Senior Social and Environment Officer | 0911307406 | Fetsum2009@gmail.com |
| **8** | Banchiayehu Eshetu | Development Bank of Ethiopia-DBE | Acting Manager M and E | 0912600228 | Maedotd4@gmail.com |
| **9** | Abiyot Bayou (Ph.D | **MInT** | Director General Digital Transformation Program (DTP) | 0911034508 | Abiyot.bayou@mint.et.gov |
| **10** | Abate Getenet | **F/EPA** | Head for Pollution Control Dpt. | 0933625098 | Abex-get@yahoo.com |
| **11** | Ato Million H/Mcheal | Ethiopian Communication Authority (ECA) | Deputy Director General | 0911105971 | milata19@gmail.com |
| 12 | Ato Tollosa | F/EPA | Head ESIA Department | 0913754227 |  |
| 13 | Zelalem Assefa (Ph.D) | EthERNet (MoE) | Director General | 0911791462 | zelalem@ethernet.edu.et |
| 14 | Mesfin Belachew (Ph.D) | Project Coordinator for Ethiopia Digital Foundations Project (EDFP) | MInT/PIU |  | Mesfin.belachew@mint.edu.et |
| **No** | **Name** | **Office** | **Position** | **Cell No** | **Email** |
| **Regional Level** |
| **Afar** |
| **15** | Abdo Hannatu | Afar-Science, Innovation and Technology Commission | Director-ICT | 0904341924 | Abdi2016@gmail.com |
| **16** | Tewoled Birhan | Afar-Science, Innovation and Technology Commission | Team Leader-ICT | 0911540154 | Tewoled54@gmail.com |
| **17** | Amina Musa | Afar-BoWSA | Director | 0911040974 | aminamussa2013@gmail.com |
| **18** | Seadan Ahmed | Afar-BoWSA | Women Right Protection Unit Leader | 0914118914 |  |
| **19** | Fatuma Nuru | Afar-BoWSA | Capacity Building Unit Leader | 0942789716 | Fafinjor2022@gmail.com |
| **20** | Abdulkadir Mohamed | EPA | Director | 0913084083 |  |
| **21** | Mohamed Awol Ebrahim | Peace and Security | Director |  |  |
| **22** | Mohamed Ahmed | Trade & Industry | Director |  |  |
| **Somali** |
| **23** | W/ro Fatuma Mohamed | MInT | Head  |  |  |
| **24** | Ubha Abduirahaman | Women and Child Affair | Deputy Head |  |  |
| **25** | Mohamed Adem Ibrahim | EPA | Deputy Head |  |  |
| **26** | Mohamed Hassen Ahmed | MInT | Deputy Head | 0911661461 | Maxamund52@gmail.com |
| **27** | Abdi Yesuf Mohamed | EPA | Planning Director | 0915210499 | abdiyew@gmail.com |
| **28** | Mohamed Ali Ibrahim | MInT | Product and engineering service | 0915061840 | Moali4002@gmail.com |
| **29** | Kaswal Abdi Ahmed | MInT | HR director | 0915634049 | Qabulabdi32@gmail.com |
| **30** | Ahmed Mohamed Abdi | MInT | Research and Award Director | 0915077794 | Dhorabkiliye222@gmail.com |
| **31** | Abdi Nasir Mohamed | BoWCA |  | 0915051788 | Abdnasir8485@gmail.com |
| **32** | Abdulfeta Amir Abdi | EPA | Climate Change Expert | 0911856504 |  |
| **33** | Abdulaziz Muhamed | BoWCA | Finance Head | 0915304295 | Gabiib999@gmail.com |
|  | Abdurahman Kamel | MInT | IT Director | 0911596487 | Abdurahmank41@gmail.com |
| **Gambella** |
| **34** | Yonas Abebe | Peace and Security bureau (Previous Head for Environment bureau) | Deputy Head | 0965023516 | yonasabebe021@gmail.com |
| **35** | Mulugeta Melkamu | Women & Social Affairs  | Bureau, Planning Director | 0918063343 | mulugeta0633@gmail.com |
| **36** | Nugus H/ Mariam | MInT | Information Systems Directorate Director | 0991442257 | nigus.hmariam@gmail.com |
| **37** | Chunna Lero | MInT | ICT Infrastructure Supply & Maintenance Directorate Director | 0935150765 | chunnalero@gmail.com |
| **38** | Tesfaye Kassa | MInT | Technology Training Directorate Director | 0935150765 | getamelkam5@gmail.com |
| **39** | Paul Gari | MInT | Commissionaire | 0944230048 | pgoduru@gmail.com |
| **No** | Name | Office | Position | Cell No | email |
| Afar Woreda Level |  |  |  |
| **40** | Fiyori Atnafe | Rural Land Administration | Engineer | 0935376025 |  |
| **41** | Ahmed Abdulkadir | Trade Office | Head | 0911664100 |  |
| **42** | Sultan Ahmed | Peace and Security Office | Head | 0912551650 |  |
| **43** | Seada Aminu | Women and Child Office | Head | 0925028187 |  |

1. The Regional Economic Communities/RECs (East African Communities/EAC and Intergovernmental Authority on Development/IGAD) will be treated under Unguaranteed Commercial Financing that is financing for RECs and countries in SOP-I, II includes both national and regional IDA allocations. [↑](#footnote-ref-1)
2. As it is indicated in the PAD, the fate opf the ECA is not decided yet. [↑](#footnote-ref-2)
3. Ethiopia is emerging from a period of internal conflict, which began in 2020, with a peace treaty signed in November 2022. [↑](#footnote-ref-3)
4. According to ESS4- GN24.5. Appropriate conduct is expected of any private security forces employed by the project. Contractual arrangements provide clear instructions on the limited circumstances in which force may be used to protect the project’s personnel or property. Adequate protocols should also be in place and implemented for security services provided by government entities. [↑](#footnote-ref-4)
5. According to ESS4- GN24.5. Appropriate conduct is expected of any private security forces employed by the project. Contractual arrange ments provide clear instructions on the limited circumstances in which force may be used to protect the project’s personnel or property. Adequate protocols should also be in place and implemented for security services provided by government entities [↑](#footnote-ref-5)
6. IGAD, IGAD Regional Strategy: Volume 1 The Framework (IGAD: Djibouti, Jan. 2019), p. 15. [↑](#footnote-ref-6)
7. IGAD (note 1), p. 9. [↑](#footnote-ref-7)
8. License Round Somalia, ‘License Round Open’; and Quartz Africa, ‘Why the US, UK, France and Norway are taking sides in Kenya’s maritime row with Somalia’, 7 Nov. 2019. [↑](#footnote-ref-8)
9. @AbdinurMAhmed, Twitter post, 22 Nov. 2019, 19:53. [↑](#footnote-ref-9)
10. Norwegian Institute of International Affairs-NUPI (June, 2022). Climate, Peace and Security Fact Sheet-Ethiopia. Contributors: NUPI, Asha Ali, Anne Funnemark, Dr ElisabethL. Rosvold; SIPRI, Dr Farah Hegazi, Dr Kyungmee Kim,Katongo Seyuba, Kheira Tarif. Visuals: Jose Luengo-Cabrera& Katongo Seyuba. Design: Winkel AS [↑](#footnote-ref-10)
11. Ibid. [↑](#footnote-ref-11)
12. De Waal, A., ‘Horn of Africa and Red Sea synthesis paper’, 2017, p. 6. [↑](#footnote-ref-12)
13. WFP (2022). Severe hunger tightens grip on Northern Ethiopia; IOM (2022). Ethiopian humanitarian response overview. [↑](#footnote-ref-13)
14. de Waal, A. (1991). Evil days. 30 years of war and famine. Africa Watch; Mussa, M. et al. (2017). Indigenous conflict management and resolution mechanisms on rangelands in pastoral areas, Ethiopia. Journal of African Studies and Development, 9(9). [↑](#footnote-ref-14)
15. Taye, B. (2017). Ethnic federalism and conflict in Ethiopia. African Journal of Conflict Resolution, 17(2). [↑](#footnote-ref-15)
16. Yarnell, M. ( 2018). The crisis below the headlines: Conflict displacement in Ethiopia. Refugees International. [↑](#footnote-ref-16)
17. Ethiopian Human Rights Commission & UNHCR (2021). Investigation into alleged violations of international human rights, humanitarian and refugee law committed by all parties to the conflict in the Tigray region of the Federal Democratic Republic of Ethiopia. [↑](#footnote-ref-17)
18. Lumborg et al., 2021; Debebe, A. (2016). Mobility and conflict: Persistent challenges in expanding access to education among pastoralists of South Omo, Ethiopia. Ethiopian Journal of Education and Sciences, 11(2). [↑](#footnote-ref-18)
19. Meier, P. et al. (2007). Environmental influences on pastoral conflict in the Horn of Africa. Political Geography, 26(6); Hagmann, T. & Mulugeta, A. (2008). Pastoral conflicts and state-building in the Ethiopian lowlands. Africa Spectrum, 43(1). [↑](#footnote-ref-19)
20. Meier et al., 2007; Lumborg et al, 2021. [↑](#footnote-ref-20)
21. Fjelde, H. & von Uexkull, N. (2012). Climate triggers: Rainfall anomalies, vulnerability and communal conflict in Sub-Saharan Africa. Political Geography, 31(7); van Weezel, S. (2019). On climate and conflict: Precipitation decline and communal conflict in Ethiopia and Kenya. Journal of Peace Research, 56(4). [↑](#footnote-ref-21)
22. van Weezel, 2019. [↑](#footnote-ref-22)
23. Raleigh, C. & Kniveton, D. (2012). Come rain or shine: An analysis of conflict and climate variability in East Africa. Journal of Peace Research, 49(1); Meier et al, 2007. Meier et al., 2007. [↑](#footnote-ref-23)
24. Meier et al., 2007. [↑](#footnote-ref-24)
25. Executive Order 14046 (September 17, 2021), https://home.treasury.gov/system/files/126/14046.pdf; AP News, US to cut Ethiopia from trade program over rights abuses (November 2, 2021), https://apnews.com/article/joe-biden-business-africaunited-states-global-trade-a3e4988 [↑](#footnote-ref-25)
26. PBS, Food aid in Ethiopia’s Tigray now at ‘all-time lowest,’ U.N. reports (January 20, 2022), https://www.pbs.org/newshour/world/food-aid-in-ethiopias-tigray-now-at-all-time-lowest-u-n-reports. [↑](#footnote-ref-26)
27. Business Insider Africa, Safaricom CEO confirms plans are still on course to continue operations in Ethiopia amid civil unrest (November 11, 2021), https://africa.businessinsider.com/local/markets/safaricom-ceo-confirms-plans-are-still-on-course-tocontinue-operations-in-ethiopia/tv314et; Business Insider Africa, As armed conflict escalates in Ethiopia, Safaricom evacuates staff (November 9, 2021), https://africa.businessinsider.com/local/markets/as-armed-conflict-escalates-in-ethiopia-safaricomevacuates-staff/ktgff61. [↑](#footnote-ref-27)
28. The East African, Safaricom wary of Addis as profit rises to $334m (November 13, 2021), https://www.theeastafrican.co.ke/tea/business/safaricom-wary-of-addis-as-profit-rises-to-334m--3617540. [↑](#footnote-ref-28)
29. World Bank and TMG. 2022. Horn of Africa Missing Links Study (P176181). [↑](#footnote-ref-29)
30. World Bank. 2022. Project Appraisal Document: Eastern Africa-Regional Digital Integration Project (P176181). [↑](#footnote-ref-30)
31. EHRC reports human rights violations, abuses by all parties to the conflict in Afar, Amhara regions (March 11, 2022). [↑](#footnote-ref-31)
32. Ibid [↑](#footnote-ref-32)
33. EHRC reports human rights violations, abuses by all parties to the conflict in Afar, Amhara regions (March 11, 2022). [↑](#footnote-ref-33)
34. EHRC reports human rights violations, abuses by Oromo Liberation Army (OLA), and the Gambella Liberation Front (GLF) militants in Oromia and Gambella regions (September 28, 2022). [↑](#footnote-ref-34)