MINISTRY OF ENERGY AND MINERALS

SOMALILAND

271.6KM, 400KV, WAJAALE-HARGEISA-BERBERA ELECTRICITY TRANSMISSION LINE SOMALILAND

SECURITY RISK ASSESSMENT AND MANAGEMENT PLAN (SRAMP)

Official Use Only

ACRONYMS

ASP	Activity Security Plan
CIMT	Critical Incident Management Team
EAPP	Eastern Africa Power Pool
EHS	Environment Health and Safety
ERI	Early Recovery Initiatives
ESF	Environmental and Social Framework
ESHS	Environmental, Social, Health and Safety
ESIA	Environmental and Social Impact Assessment
ESMF	Environmental and Social Management Framework
ESS	Environmental and Social Standards
GBV	Gender Based Violence
GIIP	Good International Industrial Practices
GoSL	Government of Somaliland
GPN	Good Practice Notes
GRMs	Grievance Redress Mechanism
HIPC	Heavily Indebted Poor Countries
IED	Improvised Explosive Device
IFC	International Finance Corporation
IGMOU	Inter-Governmental Memorandum of Understanding
IOS	International Organization for Standardization
MoEM	Ministry of Energy and Minerals
MoIFAR	Ministry of the Interior and Federal Affairs
NISA	National Intelligence and Security Agency
OHS	Occupational, Health and Safety
PIDA	Program Infrastructure Development for Africa
PIU	Project Implementation Units
RoE	Rules of Engagement
RoW	Right of Way
RPSMP	Regional Power System Master Plan
SEA	Sexual Exploitation and Abuse
SEP	Stakeholder Engagement Plan
SNA	Somaliland National Army
SNP	Somaliland National Police
SRAMP	Security Risk Assessment and Management Plan
SRM	Security Risk Model
TL	Transmission Line
UN	United Nations
UNSMS	UN Security Management System
UXO	Unexploded Ordnance
VBIED	Vehicle Born Improvised Explosive Devices
VPs	Voluntary Principles
WB	World Bank
WBG	World Bank Group

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The proposed project is a 271.3km long double circuit Extra High Voltage 500kV Transmission Line (TL); starting from proposed Togo-Wajaale and terminating at the proposed Berbera substation passing through Hargeisa. The line crosses 3 districts (Gebiley, Hargeisa and Berbera) and several villages found in the 2 regions.

The Security Risk Assessment and Management Plan (SRAMP) is prepared with objective of to assess and identify the potential security risks that could potentially threaten the safety and security of the program workers and the beneficiary community in the program intervention areas. The specific objectives are highlighted in the next sub section. Both primary and secondary data were used for the preparation of the document.

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

The World Bank's ESS1: Assessment and Management of Environmental and Social Risks and Impacts and ESS4: Community Health and Safety require the PMU to assess, manage and monitor potential social risks and impacts as a result of Horn of Africa Regional Power System Transformation Project (P179036), including threats to human security through personal, communal or interstate conflict, as well as more general crime or violence.;

1. Analyses the risks to Horn of Africa Regional Integration for Sustainable Energy Supply as a project and identifies the sources of threat and nature of risk to human security as a result of the delivery of Horn of Africa Regional Power System Transformation Project
2. Documents how risks will be mitigated during the lifetime of Horn of Africa Regional Power System Transformation Project How incidents will be managed during the project.

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

- Theft of equipment and material: employee or visitor/gust stealing equipment or material from project site or individual house.
- Burglary: Illegal entry of a building with intent to commit a crime, especially theft. It involves breaking and entering the premises. This can be done by staff or outsiders.
- Banditry/Roadside attacks on workers during transit: The project can be susceptible to attacks while transporting equipment and materials to the targeted regions or to project workers when travelling for field activities.
- Community unrest: Due to influx of labor, improper behavior towards the community, land and water use conflict, improper site selection and locating project infrastructures and associated facilities, resource abuse by the contractors, improper waste disposal, noise and dust pollution, etc.,
- Risks from employee industrial action and disruption of services: likely cause for labor disputes include demand for limited employment opportunities; labor

wages/rates and delays of payment; disagreement over working conditions, raising concerns regarding unsafe or unhealthy work situations, or any grievances raised, and such situations could lead to labor unrest and work stoppage.

- Gender-Based Violence (GBV)/sexual exploitation and abuse (SEA) and gender-based security incidents. This becomes a security issue when GBV/SEA is inflicted by perpetuators to women and girls of the project workers and community in the project areas (Please refer to the project level GBV Action Plan).
- Risks emanating from the use of security personnel: Use of security personnel may exacerbate tensions. Security personnel can be private or public. Security personnel can be engaged by the project contractor. Their presence can pose risks to, and have unintended impacts on, both project workers and local communities. Examples include committing a GBV/SEA act by security personnel within conflict affected work environment. It can also occur during community unrest and actions ethnic conflicts within the work environment.
- Risks associated with armed conflict and kidnapping: armed conflict between government and non-government forces and between non-government armed forces. In areas in which armed groups are operating, there are risk of kidnapping.
- Risk of traffic accident: due to erratic driving habits and poorly maintained road infrastructure traffic accidents are potential risks.
- Medical risk: Access to adequate medical and emergency care in rural areas of the country is limited causing medical risks.
- Exposure to natural hazard (flooding): the rainy season in Somaliland runs from June to September, and during this period flooding is common posing flooding.

1 INTRODUCTION

1.1 Project Development Objectives

The Horn of Africa Horn of Africa Regional Power System Transformation Project (P179036) is a World Bank financed project whose objective is to enhance regional integration of energy supply and to improve energy access in the borderlands in Horn of Africa countries.

1.2 Project Components

1.2.1 Component 1-Physical Interconnection Infrastructure

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

1.2.2 Component 2-Energy Access Interventions in Borderland Areas

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

1.2.3 Component 3-Technical Assistance and Capacity Building for Regional Power Integration.

Component 3 will provide technical assistance and capacity building to the EAPP, its member countries. This component will be informed by the Regional Power System Master Plan (2014) (RPSMP) of the EAPP[2] and the African Union Program Infrastructure Development for Africa (PIDA) 2020 Priority Action Plan. In addition, proposed activities will be informed by the EAPP 10-year Strategic Plan (2018–2027) and the Short-term Action Plan (2021–2023).

---

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

[2] The RPSMP is subject to update, which is expected to start in June 2021.

1.3 Project Proponents

1.3.1 Ministry of Energy and Minerals

The proponent of the proposed 271.3km double circuit High Voltage 500kV transmission line is Somaliland Ministry of Energy and Minerals (MoEM). A Project Implementation Unit (PIU) has been established at the MoEM and will be responsible for the management of the project. The PIU includes a Project Coordinator, financial management Specialist, procurement specialist, monitoring and evaluation specialist, environment specialists, social specialist and technical specialist.

1.3.2 Eastern Africa Power Pool

The Eastern Africa Power Pool (EAPP) is a regional institution established in 2005 to coordinate cross-border power trade and grid interconnection among nations of the Eastern Africa region. The EAPP currently has thirteen (13) member states that signed the Inter-Governmental Memorandum of Understanding (IGMOU) and fourteen utilities that signed the Inter Utility Memorandum of Understanding (IUMOU). The pool comprises the following countries: Burundi, Djibouti, Democratic Republic of Congo (DRC), Rwanda, Egypt, Ethiopia, Kenya, Sudan, Tanzania, Uganda, and Libya. South Sudan and Somalia joined recently and there's a possibility that Eritrea may join. The EAPP's General Secretariat is based in Addis Ababa, Ethiopia with a mandate to coordinate the development and functioning/operation of the power pool. A The PIU includes a Project Coordinator, financial management Specialist, procurement specialist, monitoring and evaluation specialist, environment specialists, social specialist and technical specialist.

1.4 Project Overview

The proposed project is a 271.3km long double circuit Extra High Voltage 500kV Transmission Line (TL); starting from proposed Togo-Wajaale and terminating at the proposed Berbera substation passing through Hargeisa. The line crosses 3 districts (Gebiley, Hargeisa and Berbera) and several villages found in the 2 regions (Table 1.2). The proposed Right of Way (RoW) for the transmission line will be a 40metre wide corridor suggesting that approximately 1,085ha. of land may be acquired and/or expropriated for project purposes. The project will require the erection of 678 steel lattice towers (tension and suspension types) spaced at average distance of 400m (depending on the terrain and stability of the soil). Tension towers will be installed in angles and suspension towers will be installed along the line as load bearing support. The salient features of the transmission line are given in Table 1-1.

Table 1-1. Project Salient Features

#	Features	Description
1	Voltage Rating	500kV
2	Type of Transmission Line	Double Circuit
3	Width of T/L Right of Way (RoW)	40m
4	Type of Line Support	Steel Towers
5	Conductor	AAAC Ash 180.7 mm^2
6	Conductor Material	Aluminum Alloy
7	Line Insulator	Disc type, Porcelain
8	Type of Connection	Substation
	Tapping point:	Wajaale
	Termination point:	Berbera
9	Number of Angle Towers	20
	Approximate number of towers to erect:	678

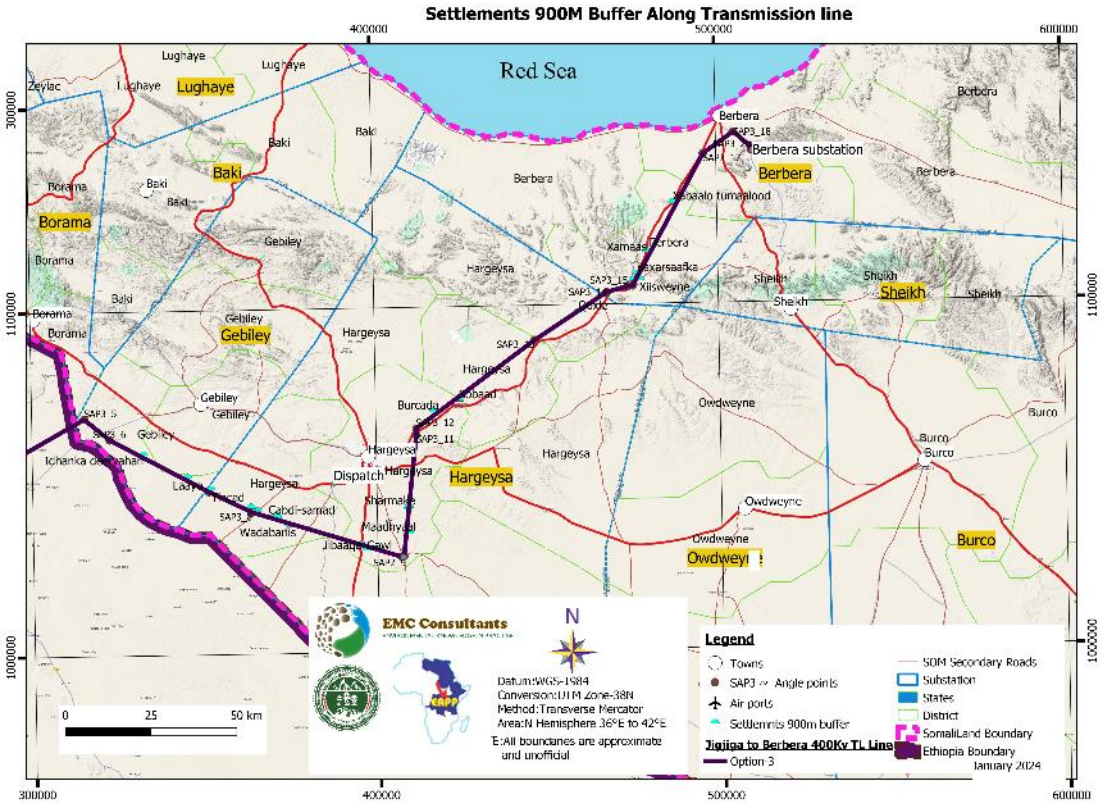
10	Average/Standard Tower Height (m)	40
11	Approximate Length of T/L	271.3
	Average span between towers over normal topography	400m
12	Total land requires for installing a typical Tower	256m^2 (16m x 16m)
13	Standard Distance between phase-to-phase conductors (approx.)	4m

Source: Feasibility Study Report

Table 1-2: Administrative Boundaries Traversed by Transmission Line

REGION	DISTRICT	AFFECTED VILLAGES
MAROODIJEH	Gebiley	Godka Carrada
		Dhagaxyo Cad1
		Laaya
		Tinad
	Hargeisa	Da'arta
		Sheekh Muhamed Yarre
		Lafta Farawayne
		Aw-Barre
		Sheikh Mooldhe
		Carra Madow
		Shirwareen
		Ina Cunaaye
		Jibaaqe
		Galoole
		Sharmaarke
		Maadhyaal
		Markazka-Burcada Yar
		Aw-Barkhadle
		Dacar Budhuq
SAHIL	Berbera	Lafaruug
		Laas Geel
		Xabaalo Tumaalood
		Baxarasaafka

Figure 1-1: Transmission Line Route



Source: EMC Consultants, 2024

Upon completion, the 500kV double circuit transmission line will be energized as part of the national grid and will be part of the Ethiopia-Somaliland interconnector.

1.5 Security Risk Assessment Objective

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

1.5.1 Specific Objectives

- Identify potential security risks due to intentional and unintentional threats that have a potential for direct or indirect consequences on the proposed electricity project activities, assets, individual workers, community, and other stakeholders.
- To identify, evaluate, and prioritize potential security risks and impacts likely to affect the safety and security of persons and operation of the project;
- To understand to community concerns and perceptions
- To determine appropriate security arrangements
- Systematically evaluate and prioritize security risks controls and mitigation measures.
- Systematically analyze potential risks (its likelihood and consequence analysis).
- Determine those potential risks that have significant adverse impact on the activities of the proposed electricity project, contractors, subcontractors, assets, workforce, and local communities.
- Screening out extremely high-risk areas, with a phased approach allowing reassessments and potential integration of areas where the situation improves over

time.

1.6 Security Management Plan Objective

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

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

1.6.1 Specific Objectives

- To determine appropriate security arrangements
- To define the required resources for the identified actions of the project
- To assess and define the responsible actors, institutions and agencies for the planning and implementation of the
- Systematically evaluate and prioritize security risks controls and mitigation measures.

1.6.2 Security Risk Assessment Methodology and Scope

1.6.2.1 Scope

The assessment focusses on the areas that the transmission line crosses i.e. 2 Regional Member States including 3 districts (Gebiley, Hargeisa and Berbera) and several villages found in the 2 regions (Table 1-2).

1.6.2.2 Literature Review

Secondary data was reviewed as part of the preparation of the security risk assessment and management plan. Secondary data such as review of relevant national legislation and regulations, Good International Industrial Practices (GIIP) for instance ISO 31000 (Risk Management Guidelines) and the WB Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel. Additionally, research findings on the country's security situation were also reviewed and utilized.

1.6.2.3 Interviews

Interviews were conducted with various stakeholders, including communities living in the area, religious leaders, local elders, government security bodies such as the police, and relevant government ministries. These interviews aimed to gather insights and perspectives on the existing security conditions.

2 LEGAL FRAMEWORK

2.1 National Polices and Legal Frameworks

2.1.1 Provisional Constitution of Somaliland

Article 24: The Right to Life, Security of the Person, Respect for Reputation and Crimes against Human Rights

- Human life is the gift of Allah and is beyond price. Every person has the right to life and shall only be deprived of life if convicted in a court of an offence in which the sentence laid down by law is death.
- Every person shall have the right to security of his person. Physical punishment and any other injury to the person is prohibited.
- Every person shall have the right to have his dignity, reputation and private life respected.
- Crimes against human rights such as torture, extra-judicial killings, mutilation and other similar acts shall have no limitation periods.

Article 25: The Right to Liberty, Guarantees and the Conditions of Rights and Freedoms

- No person shall be deprived of his liberty except in accordance with the law.
- No person may be arrested, searched, or detained, except when caught *in flagrante delicto*, or on the issue of a reasoned arrest warrant by a competent judge.
- The state shall guarantee to all citizens their rights and freedoms and the punishment for any of their infringements shall be determined by law.
- The freedoms of the person shall not override the laws protecting the public morals, the security of the country or the rights of other individuals.

2.2 World Bank Environmental and Social Framework Requirement

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

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

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

Relevance: “Annex 1 5(e) Social and conflict analysis is an instrument that assesses the degree to which the project may (a) exacerbate existing tensions and inequality within

society (both within the communities affected by the project and between these communities and others); (b) have a negative effect on stability and human security; (c) be negatively affected by existing tensions, conflict and instability, particularly in circumstances of war, insurrection and civil unrest."

2.2.2 ESS4: Community Health and Safety

ESS4 recognizes that project activities, equipment design and safety, infrastructure, and safety services can increase community exposure to risks and impacts. It also addresses Infrastructure and equipment design and safety and safety of services which involves provision of services to communities and the corresponding responsibility of borrowers to avoid or minimize such risks and impacts. In particular, in conditions where the borrower[3] through the Project Implementation Unit (PIU) engage direct or contracted workers to provide security to protect project workers and assets, ESS4 require to assess the risk posed by the security arrangements within and outside the project site. Besides, the standard states the borrower is expected to ensure that government security personnel deployed to give security services act guided by the principles of proportionality and GIIP. Furthermore, the standard requires the borrower to verify and ensure the direct and contracted workers engaged to give security did not induce abuse. Moreover, ESS4 demands the borrower to review and take corrective measures for all accusations inappropriate doings of the security personnel.

2.2.3 World Bank Group Environment, Health and Safety (EHS) Guidelines

World Bank Group (WBG) Environment, Health and Safety (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 emergency preparedness plans and relevant applicable management practices. 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.

2.3 International Standards and Good Practice

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

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

[3] Somaliland Government

- UN Code of Conduct for Law Enforcement Officials
- Voluntary Principles (VPs) on Security and Human Rights
- http://www.voluntaryprinciples.org/what-are-the-voluntary-principles
- International Code of Conduct for Private Security Service Providers. https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF CONDUCT-Amended_2021.pdf
- International Finance Corporation (IFC) Handbook on the Use of Security Forces: Assessing and Managing Risks and Impacts, 2017 (available in English, French, Spanish)
  https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_s it e/sustainability-at-ifc/publications/publications_handbook_securityforces

2.3.1 ISO 31000 Risk Management Guidelines

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

3 SECURITY CONTEXT AND RISK ASSESSMENT

3.1 National Security Context

Somaliland declared independence from Somalia in 1991 and does not consider itself affiliated with the Federal Government of Somalia (FGS)[4]. It continues to arrest and detain persons critical of independence as well as residents who are employed by the FGS.[5] Somaliland's borders were not formed along clan lines, and its territory comprises areas inhabited by Dir sub-clans, such as Ciise and Gadabuursi, the Isaaq, which are the dominant clan and constitute almost two-thirds of the population, and the Harti sub-clans the Dhulbahante and Warsangeli along the border with Puntland. Minority groups present in Somaliland include Gaboye, Tumal and Yibir. Somaliland continues to lobby for international recognition as an independent State. While Somalia and Somaliland have previously engaged in diplomatic talks, these faltered during 2021.

Somaliland has its "own civilian administration, armed forces and currency, and it runs its own elections." Despite some concerns about police actions during campaigning, and despite long delays, Somaliland held free and fair elections on 31 May 2021 for parliamentary and local council positions.

The opposition Waddani party won the majority of seats in the House of Representatives and other key local positions and formed a controlling coalition with the Justice and Welfare Party (UCID), another opposition party. While one Gabooye candidate was elected to a parliamentary seat, which was considered a step towards minority representation, no women were elected. Presidential elections are scheduled for November 2022. Allegations from opposition parties that the President intended to extend his term and delay the elections sparked protests in August 2022.

Somaliland has not suffered a successful terrorist attack in the region since 2008, but there is a consistent threat. The understanding is that this threat is in relation to the Government of Somaliland (GoSL) expressing sympathies for the death of General Galal during the January 2021 al-Shabaab attack on Afrik Hotel in Mogadishu. This threat, specifically against large cities in Somaliland, has increased the overall threat level for the majority of the region.

Other issues in Somaliland include the rise of sexual violence and rape cases, clan conflicts and a reduction of civil liberties. Two opposition party candidates were arrested in Hargeisa

[4] See, for example, Heritage Foundation, Somalilanders' Quest for Independence Isn't "Neocolonial" Plot. It's Self-Determination., 9 May 2022, www.heritage.org/africa/commentary/somalilanders-quest-independence-isnt-neocolonial-plot-its-self-determination.

[5] "Somaliland authorities continued to detain Somaliland residents employed by the federal government in Mogadishu, sometimes for extended periods. Somaliland authorities did not authorize officials in Mogadishu to represent Somaliland within or to the federal government and viewed such actions as treason, punishable under Somaliland law." US Department of State, *2021 Country Report on Human Rights Practices: Somalia*, 12 April 2022, www.ecoi.net/en/document/2071126.html. See also, Somaliland Human Rights Center, Annual Report of Human Rights Center 2021, 12 February 2022, http://hrcsomaliland.org/wp-content/uploads/2022/02/Annual-report-2021.pdf, pp. 13-16; All Africa, Somalia: Former Deputy Somali PM Arrested in Hargeisa, 15 December 2021, https://allafrica.com/stories/202112160116.html; Somaliland Standard, SL Police Detain 50 Youth for Wearing the Attire Flag of Somalia in Borama, 27 June 2021, https://somalilandstandard.com/sl-police-detain-50-youth-for-wearing-the- attire-flag-of-somalia-in-borama/; Italian Institute for International Political Studies, *Somaliland: 30 Years of De Facto Statehood, and No End In Sight*, 12 May 2021, www.ispionline.it/en/pubblicazione/somaliland-30-years-de-facto-statehood-and-no-end-sight-30363; All Africa, Somalia: Somaliland Releases Detained Musicians, 24 June 2020, https://allafrica.com/stories/202006250225.html; Somali Dispatch, *Somaliland: Singer Salah Arab Released from Detention*, 11 May 2020, www.somalidispatch.com/latest-news/somaliland-singer-salah-arab-released-from-detention/.

in February 2021, and a social media figure was detained without charge for two months in late 2020.

The issue which connects both Somaliland and Puntland is that of the disputed regions of Sool and Sanaag, which results in frequent skirmishes between their two respective security forces. Fighting in Tukaraq in Sool, is commonplace, and resulted in a number of deaths in 2018.There have been instances reported of Puntland soldiers also defecting to Somaliland, and vice versa, which highlights the ongoing complexity of the relationship between the two regions.

3.1.1 Clan Clashes

Clashes between Habar Yonis/Sa'ad Yonis and Habar Je'lo/Bi'de sub-clans in El Afweyne in the Sanaag region of Somaliland have persisted for many years[6]. On 10 March 2020, following an agreement by traditional and religious leaders, the two rival sub-clans began an exchange of compensation for victims of the conflict. When an inter-clan conflict between Reer Hagar and Hayaag in the Togheer region resulted in the killing[7] of a Hayaag man in 2019, it sparked a cycle of revenge violence, costing 27 lives in less than one year,until mediation ended the dispute and ordered compensation. In April 2021, a conflict between Dhulbahante sub-clans Jama Siyaad and Ugaadhyahan/Naaleeye Ahmed in the Sool region caused at least 15 deaths; peace negotiations were ongoing as of June 2021. Dhulbante clan members clashed with Habar Je'lo members in April 2021 in the Togdheer region, causing at least four deaths[8].

"President Bihi's administration [in Somaliland] has faced a recurrent inter-clan conflict in Ceel Afweyn, in Sanaag region, that pits two major branches of the Isaq clan-Bicido/Habar Jeclo and Saad Yonis/Habar Yonis-against each other. The conflict's roots lie in a long-running Habar Jeclo versus Habar Yonis feud that intensified during the 2017 election, which Bihi, backed by a Habar Jeclo-led alliance, won." ICG, *Averting War in Somalia*, 27 June 2018, www.crisisgroup.org/africa/horn-africa/somaliland/141-averting-war-northern-somalia.

3.2 Security Situation in Districts Traversed by Transmission Line

Somaliland has not suffered a successful terrorist attack in the region since 2008, there is a consistent and current threat at the time of writing. The understanding is that this threat is in relation to the Government of Somaliland (GoSL) expressing sympathies for the death of General Galal during the January 2021 al-Shabaab attack on Afrik Hotel in Mogadishu. This

---

[6] "President Bihi's administration [in Somaliland] has faced a recurrent inter-clan conflict in Ceel Afweyn, in Sanaag region, that pits two major branches of the Isaq clan – Bicido/Habar Jeclo and Saad Yonis/Habar Yonis – against each other. The conflict's roots lie in a long-running Habar Jeclo versus Habar Yonis feud that intensified during the 2017 election, which Bihi, backed by a Habar Jeclo-led alliance, won." ICG, *Averting War in Somalia*, 27 June 2018, www.crisisgroup.org/africa/horn-africa/somaliland/141-averting-war-northern-somalia.

[7] "As of June 2021, four men (two Dhulbahante and two Habar Je'lo) were killed." EASO, *Somalia: Targeted Profiles*, 20 September 2021,www.ecoi.net/en/file/local/2060580/2021_09_EASO_COI_Report_Somalia_Targeted_profiles.pdf, p. 80

[8] "The bone of contention was a well. The fighting left 18 men dead, including 15 from the Ugaadhyahan sub-clan and 3 from the Jaama Siyaad […]Peace negotiations are ongoing (as of June 2021)." EASO, *Somalia: Targeted Profiles*, 20 September 2021, www.ecoi.net/en/file/local/2060580/2021_09_EASO_COI_Report_Somalia_Targeted_profiles.pdf, p. 79. See also, Somali Affairs, *Casualties in Clan Clashes in Sool*, 16 April 2021, www.somaliaffairs.com/news/somalia-casualties-in-clan-clashes-in-sool/; UN Security Council, *Letter Dated 5 October*, 6 October 2021, S/2021/849, www.ecoi.net/en/file/local/2062553/S_2021_849_E.pdf, para. 32

threat, specifically against large cities in Somaliland, has increased the overall threat level for the majority of the region. Other issues in Somaliland include the rise of sexual violence and rape cases, clan conflicts and a reduction of civil liberties. Two opposition party candidates were arrested in Hargeisa in February 2021, and a social media figure was detained without charge for two months in late 2020.

3.2.1 Maroodijeh Regional Administration

3.2.1.1 Security Situation in Gebiley District

The figure below shows the distribution of incidents in the Gebiley District over the last 12 months. The table 3-1 shows the number of incidents for each determined category over the last 12 months.

Table 3-1: Incidents in Gebiley District 2024

Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Extremist Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0
IEDs	0	0	0	0	0	0	0	0	0	0	0	0	0
Communal Violence	0	2	0	4	0	0	1	3	0	0	0	0	10
Criminal Activity	0	1	0	4	5	1	2	1	0	1	7	3	25
Security Operations	0	0	0	0	0	0	0	0	0	0	0	0	0

Source: EMC Consultants, 2024

3.2.2 Security Situation in Hargeisa

In Hargeisa, the capital city of Somaliland, a high percentage of its population is subject to physical insecurity, with rampant street crime, frequent disputes over land and buildings, a proliferation of weapons, and increasing youth gang problems. Unemployment and clan-related tensions increase insecurity, and women are vulnerable to robbery and rape. This insecurity is exacerbated by an influx of immigrants to the city including IDPs affected by conflict, individuals fleeing conflict in Yemen, and members of the diaspora returning from abroad. The result of this is that physical security is pursued in a reactive fashion, rather than a pre-emptive pursuit of human security. The table 3-2 shows the number of incidents for each determined category over the last 12 months.

Table 3-2. Incidents in Hargeisa District in 2024

Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Extremist Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0
IEDs	0	0	0	0	0	0	0	0	0	0	0	0	0
Communal Violence	1	0	0	0	0	0	0	0	0	0	0	0	2
Criminal Activity	0	3	2	1	6	1	6	3	4	1	1	4	32
Security Operations	0	0	0	0	0	0	0	0	0	0	0	0	0

Source: EMC Consultants, 2024

3.2.3 Sahil Region

3.2.3.1 Security Situation in Berbera District

The security situation in Berbera, Somaliland, is generally considered stable, despite some ongoing regional tensions. The table 3-3 below shows the number of incidents for each determined category over the last 12 months.

Table 3-3. Incidents in Berbera District in 2024

Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Extremist Attacks	0	0	0	0	0	0	0	0	0	0	0	0	0
IEDs	0	0	0	0	0	0	0	0	0	0	0	0	0
Communal Violence	0	0	0	0	0	0	0	0	0	0	0	0	0
Criminal Activity	2	4	1	10	8	15	9	1	10	2	5	7	74
Security Operations	0	0	0	0	0	0	0	0	0	0	0	0	0

Source: EMC Consultants, 2024

3.3 Approach to Risk Assessment

3.3.1 Risk Criteria

To provide a common frame of reference and to ensure a consistent approach to evaluating risk within Horn of Africa Regional Integration for Sustainable Energy Supply project, we will use the risk criteria detailed in the table below. The criteria defined will be used to assess risk throughout Horn of Africa Horn of Africa Regional Power System Transformation Project in both project and district level security risk assessments.

Table 3-4. Risk Criteria

	LIKELIHOOD					
IMPACT		1	2	3	4	5
	5	Moderate	High	High	Extreme	Extreme
	4	Low	Moderate	High	High	High
	3	Low	Moderate	Moderate	High	High
	2	Low	Low	Low	Moderate	Moderate
	1	Negligible	Negligible	Negligible	Negligible	Negligible

IMPACT CRITERIA	
5	Exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes or functions, or irreparable damage to reputation.
4	Serious consequences, such as loss of life or serious injuries, impairment of core processes and functions for an extended period of time, or serious reputational damage.
3	Moderate to serious consequences, such as injuries, impairment of core functions and processes, and some reputational damage.
2	Moderate consequences, such as minor injuries, minor impairment of core functions and processes, or slight reputational damage.
1	Loss or damage of project assets would have negligible consequences or impact.
LIKELIHOOD CRITERIA	
5	Highly Likely (For example, occurs or has occurred once per 7 days) or is considered likely to occur in the near future.
4	Likely (For example, occurs or has occurred once per 30 days) or has the potential to occur in the near to mid-term future.

3	Possible (For example, occurs or has occurred once per 90 days) or is assessed to have the potential to happen in the future.
2	Unlikely (For example, occurs or has occurred once per 180 days) but possibility of occurrence in the future cannot be discounted.
1	Rare (For example, occurs or has occurred once per 365 days) and is highly unlikely to happen in future.

Source: EMC Consultants, 2024

3.4 Risk Appetite

This is the project's Risk Appetite.

ISO31000:2018 defines risk appetite as "the amount and type of risk that an organisation is prepared to pursue, retain or take".

Based on a review of available documentation and meetings, we assess the Risk Appetite of the project as follows;

Any Risk that could lead to the death or injury of Project Personnel or Project Beneficiaries is unacceptable.

3.5 Project Stakeholders

The project will not take place in a vacuum and it is anticipated that the project will feature a range of stakeholders both internal and external, including those supportive of the project and those opposed to the project. The Project SEP provides a detailed outline of the Stakeholder Identification, Mapping and Analysis processes, along with their categorization.

3.5.1 Project Workers

Project workers are all personnel from the categories identified in World Bank ESS2: Labor and Working Conditions and the Labour Management Procedures **(see project LMP report)** these are;

- **Direct Workers.** People employed directly on the Project, such the PIU, FMS, to work specifically within the Project. This category also includes any personnel directly contracted by Government of Somaliland or Ministries or entities at various project sites within the Government of Somaliland, regions and districts.
- **Contracted Workers.** They include staff from the Security Risk Management Company and Contractors, who will be contracted to support the construction of the transmission lines and substations. People engaged through third parties to perform work on the project, regardless of location. Under this category are included, employees of any non-governmental implementers, including, if used, international or national NGOs, CSOs or contractors.

3.5.2 Project Affected Parties

In addition to the project workers identified above which, broadly speaking, fit into either the Project Affected Parties or Other Interested Parties categories identified in the project level Stakeholder Engagement Plan (SEP), there are other parties on who the impact of project delivery must be considered. As part of this Security Risk Assessment, the potential impact on these Project-Affected Persons has been considered and include anyone who is affected by the Project in any way and who could be put in harm's way through Project activities.

3.5.3 Security Stakeholders

Security stakeholders are organisations which will provide support to the project and protect project stakeholders and assets from threats. This category includes Somaliland police force, custodial corps, coastal guards, Ministry of Defence (MOD), Somaliland national armed forces, traditional elders and the National Intelligence Agency (NIA) and Private Security Providers (PSP).

3.5.4 Threat Actors

Threat actors are those who pose a security or safety threat to the other categories of stakeholders involved in the project. Threat actors may not always be acting from malicious motives, for example workers who create a safety risk to others by not following mandated procedures. However, this category also includes those who seek to prevent progress in Somaliland and for who the gains delivered by the project pose a threat. The main threat actors include communal armed groups, criminal groups, extremist groups and individuals or groups with vested interests.

3.5.5 Summary of Stakeholders

Table 3-5 builds on the stakeholders identified in the SEP along with the threat actors we have assessed as potentially influencing the project.

Table 3-5. Project Stakeholders

Stakeholder Category	SEP Stakeholder Group
Community	Communities that will receive support from the project
Government of Somaliland Ministries	Ministry officers at the Government of Somaliland
	Ministry officers at the regional State and District levels
Government Bodies	Ministry of Finance Development
	Ministry of Employment, Social Affairs and Family
	Ministry of Environment and Climate Change
	Ministry of Energy and Minerals
	Ministry of Interior
	Ministry of Planning and National Development
NGOs	International and Local NGOs
	Community-Based Organisations
Institutional Stakeholders	World Bank, EU, AfDB,
Local Government Authorities	Municipal and District Councils, along with relevant officials such as District Commissioners, District Officials and other commissioners.
UN Agencies, INGOs and Donor Groups	UNDP, UN-HABITAT, United Nations Office for Project Services, International Organization for Migration, ADRA, UNHCR, ILO, UN WOMEN, Norwegian Refugee Council, World Vision International, Danish Refugee Council, European Union and USAID, UNICEF, Care, SCI, Concern International,
Security Stakeholders	Somaliland Police Force
	Custodial Corps
	National Intelligence Agency/NIA
	Coastal Guards
	Somaliland National Armed Forces
	Traditional elders
	Private Security Providers
Non-State Actors	Armed Communal Groups
	Criminal Groups

	Extremist Groups
	Vested Interest Groups

Source: EMC Consultants, 2024

3.6 Project Assets

The delivery of project will require the design and construction of transmission line. The process of delivering the project will require the transport and use of construction equipment.

3.6.1 Assets Delivered by Project

To achieve the objectives of Components 1 and 2 will require the delivery of construction equipment and materials to the identified worksites. These will include.

- The movement of construction supplies, likely to include cement, aggregate, bricks, paint, plaster, electrical wiring and lights etc.

These assets will need to be transported across Somaliland to the target locations where they will be used in the construction of the transmission line. These assets may, therefore, prove vulnerable at a number of points both in transit and during the construction process.

3.6.2 Assets Needed to Deliver Project

In addition to the assets that must be delivered and used in the construction process, there is also a requirement for equipment needed to conduct delivery and construction. These includes;

- Transport vehicles, such as articulated lorries and smaller trucks, it may also include cars and buses needed to deliver workers.
- Construction machinery, such as diggers, drilling units, cement mixers, dump trucks and cranes.

3.6.3 Assets Affected by Project Activities

The third type of assets that must be considered at risk are those which do not play a part in project delivery but may be impacted. These assets include;

- Civilian housing in close proximity to project site.
- Civilian housing located on routes taken by deliveries for project sites.

4 SECURITY RISK ASSESSMENT

4.1 Security Risk Assessment Methodology

The Security Risk Assessment has been conducted using the methodology described in section 1.6.2. The Risk Assessment process combines three distinct steps that use the information documented in Section 1. The steps are;

1) Risk Identification.
2) Risk Analysis.
3) Risk Evaluation.

The end result of the Security Risk Assessment process will be the initial Security Risk Register which will form the basis for the creation of the Project Security Management Plan (SMP).

ISO31000:2018 defines risk as "the effect of uncertainty on objectives". A more nuanced definition, also provided in the standard, is "Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood." Risk Assessment is thus built around the following formula:

Risk = Asset + Source + Event + Vulnerability + (Likelihood x Impact) Expressed in other terms a Risk requires:

1) Asset – who or what is affected by a Risk. .
2) Source – who or what causes the Risk. This includes stakeholders, project activities or the natural environment.
3) Event – what the Source of Risk does. This includes violent attacks, natural events or organizational events.
4) Vulnerability – factors that combine to permit the Risk. This can include how the project operates and the activities it conducts; it may include site or procedural weaknesses.
5) Likelihood – is how likely a Risk is to occur.
6) Impact – is how much the Risk will affect the project.

The Risk Assessment phase maps the relationship between Source + Event + Vulnerability against the Likelihood and Impact that were already identified as Risk Criteria.

4.2 Threats to Project

Based on the activities, stakeholders, assets and locations identified in Section 1: project context, there are a number of potential threats to the project. To streamline the risk assessment and management process we will categories threats into seven categories.

Table 4-1. Threats to the Project

Threat Category	Description
Cultural	Project activities will take place in a wide area of Somaliland. There is potential risk that communities may not understand the project, or see its benefits, or that project workers may offend communities. Cultural incidents could therefore prevent works from happening or escalate into attacks on the project (and its personnel).
Safety	The project is, at its heart, a construction project. Project Personnel will be working with construction works. During the project beneficiaries will also potentially be exposed to safety and construction risks.

	Safety Risks include; • Travel (by road and air) • Electrical accidents • Construction risks • Confined space working (during transmission network works) • Falls from height • Disease outbreaks/medical incidents • Disposal of construction waste
Criminal	The project (its workers, communities it takes place in, and beneficiaries) are at risk of criminal activity triggered by the project. During project activities, which include travel as well as construction works, project personnel may be targeted by criminal groups who seek to profit. Criminal activities includes; • Theft of assets • Kidnapping • Extortion • Sexual and Gender Based Violence by Project Personnel, within the project community or during travels. • Illegal checkpoints set up by armed communal militia or rogue security forces members
Extremist	The project (its workers, communities it takes place in, and beneficiaries) are at risk of attack by extremist groups. Attacks by extremists include; • Direct Fire (Assassinations or Attacks by Groups of Gunmen) • Indirect Fire (Mortar Attacks) • Improvised Explosive Devices (Static, Magnetic, Person Borne and Vehicle Borne) • Kidnapping (To prevent activities or for propaganda)
Communal Violence	The project takes place across a wide area of Somaliland. During the project there is potential for communal based violence to take place near project locations. Communal violence may also be triggered by activities where one communal group feels they have been discriminated against or have not benefitted from the project. Communal fighting is often highly violent and indiscriminate, which risks project personnel and communities being caught in the crossfire.
Vested Interests	Somaliland's business landscape straddles a complex political economy. Utilities and energy in particular, are generated, distributed and managed against this contested background, which involves explicit and implicit competition between various business, government and traditional stakeholders. The project provides both an opportunity to invest in and improve existing infrastructure and services but may also fundamentally transform business models that currently thrive on monopolistic practices.
Security Operations	The project takes place in areas of Somaliland where the security forces are actively engaged in countering the activities of non-state armed actors including communal militias, extremist organisations and criminal groups. While the security forces will not actively target the project, there may be unfortunate occasions where their actions to protect Somalis inadvertently pose a risk to the project, project personnel, communities and assets. Such actions can also include the potential risk to locations, personnel, beneficiaries and assets posed by security personnel assigned to protect project locations or assets. Note: this risk does not include illegal actions by security personnel (those are covered under Criminal Activity or Communal Violence).

Source: EMC Consultants, 2024

Note: The project will track seven categories of threats (as outlined in Table 4-2), when having mapped incidents but documents six categories. These correlate as follows:

Table 4-2. Threat Categories and Mapping

Threat Category	Map Category	Rationale
Political	Not mapped as a separate category	Political/relationship issues as opposed to an act of violence/potential violence. If political threats escalate to violence, they are tracked under communal violence markers.
Cultural	Not mapped as a separate category	Cultural relationship issues as opposed to an act of violence/potential violence. If cultural threats escalate to violence, they are tracked under communal violence markers.
Safety	Mapped as 6 - Safety Incident	The lack of nationwide monitoring makes providing comprehensive, illustrative data impossible.
Criminal	Mapped as 4 - **Criminal Activity**	Mapped as criminal activity
Extremist	Mapped as 1–**Extremist Violence OR** Mapped as 2 – **IED**	Separated to track different impacts/ threats of Direct/Indirect fire attacks by extremists and IEDs
Communal Violence	Mapped as 3–**Communal Violence**	Mapped as communal violence
Vested Interests	Mapped as 3–**Communal Violence**	Mapped as communal violence due to crossover links between Communities and Vested Interest groups.
Security Operations	Mapped as 5–**Security Operations**	Mapped as security operations except where the incident is illegal when it will be mapped as 3-Communal Violence OR 4 – Criminal Activity

Source: EMC Consultants, 2024

4.3 Vulnerability

The concept of vulnerability is critical to a nuanced view of risk; however, in the case of worksites, it is, at the pre-construction stage, sufficient to assume a potentially high level of vulnerability that will be managed due to the construction process. For Component 2 activities, given that these include a range of activities in, as yet, unknown locations we must also assume a high level of vulnerability is inherent in the activity with a view that this will become clearer, and manageable, during the delivery of these activities.

4.4 Security Risk Registers

4.4.1 Overview

The risk registers contained in this section are initial assessments only based on existing research and background knowledge. They are divided according to project components and sub-divided into Risks to worksites/activities; risks to movement, risks to population and Risks to Staff. Components 1 and 2 are, as outlined in Section 1: project context where the construction will take place.

4.4.2 Maroodijeh

4.4.2.1 Gebiley District

Table 4-3: Gebiley District Risk Register

Threat Target	Political	Cultural	Safety	Criminal	Extremist	Communal Violence	Vested Interests
Worksite	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Movement	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Population	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Staff	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

4.4.2.2 Hargeisa District

Table 4-4: Hargeisa District Risk Register

Threat Target	Political	Cultural	Safety	Criminal	Extremist	Communal Violence	Vested Interests
Worksite	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Movement	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Population	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Staff	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

4.4.3 Sahil

4.4.3.1 Hargeisa District

Table 4-5: Hargeisa District Risk Register

Threat Target	Political	Cultural	Safety	Criminal	Extremist	Communal Violence	Vested Interests
Worksite	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Movement	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Population	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Staff	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

5 SECURITY MANAGEMENT PLAN

The security measures outlined are intended to be preventative in nature and set out to mitigate a risk by reducing vulnerability and the likelihood of a risk event occurring. This is accomplished by a range of measures, as detailed below, that include a combination of procedures, assets, training and services.

5.1 Security Governance and Responsibilities

The project is a complex project, taking place in a highly dynamic environment. To adequately manage risks to the project, project personnel, assets and the communities in which the project takes place, a robust security framework is required.

5.1.1 World Bank Environmental and Social Framework

The World Bank, as mentioned above, sets out a number of requirements for borrowers that are documented in the Environmental and Social Framework. Of particular relevance for security governance in the project are the Environmental and Social Standards (ESS) and Good Practice Notes (GPN) listed below:

ESS1: Assessment and Management of Environmental and Social Risks and Impact – This standard sets out the Federal Government's responsibilities for assessing, managing, and monitoring environmental and social risks and impacts associated with each stage of a project supported by the Bank through Investment Project Financing, in order to achieve environmental and social outcomes consistent with the Environmental and Social Standards (ESSs).

ESS2: Labor and Working Conditions–This standard recognizes the importance of employment creation and income generation in the pursuit of poverty reduction and inclusive economic growth. Borrowers can promote sound worker-management relationships and enhance the development benefits of a project by treating workers in the project fairly and providing safe and healthy working conditions

ESS4: Community Health and Safety–This standard recognizes that project activities, equipment, and infrastructure can increase community exposure to risks and impacts. In addition, communities that are already subjected to impacts from climate change may also experience an acceleration or intensification of impacts due to project activities**.**

ESS10: Stakeholder Engagement and Information Disclosure–This standard recognizes the importance of open and transparent engagement between the Borrower and project stakeholders as an essential element of good international practice. Effective stakeholder engagement can improve the environmental and social sustainability of projects, enhance project acceptance, and make a significant contribution to successful project design and implementation**.**

GPN: Addressing Sexual Exploitation and Abuse and Sexual Harassment (SEA/SH) in Investment Project Financing involving Major Civil Works – This GPN sets out how the risks of sexual and gender-based violence should be assessed, addressed and responded to and is critical in meeting the requirements of ESS1 and ESS4.

GPN: Assessing and Managing the Risks and Impacts of the Use of Security Personnel – This GPN sets out the expectations on how the risks of using security personnel, something

that is likely for the project, should be assessed and managed to prevent risk to communities where works are taking place.

GPN: Road Safety – This GPN sets out the expectations on how the risk of road traffic accidents to project personnel and communities in which the project is taking place can be assessed and managed.

Activity Security Plans-Will be created by contractors hired to deliver under the project. These will outline how the security management measures outlined in the District Security Risk Assessment and Management Plans are implemented at the construction sites.

5.2 Security Responsibilities

In the Security Risk Assessment, detailed policy environment that governs security in the project has been described. It is important, however, to set out who is responsible for security and how the different organisations should interact.

Table 5-1: Security Responsibilities

PIU	Construction Contractors
• Contract and oversee the work of the Security Risk Management Company • Engage a PIU Security Advisor • Ensure the development of Project wide and District SRA in line with the requirements of and ISO 31000 • Ensure the development of a Project-wide SRAMP and District level SRAMP, and project level Activity Security Plan (ASP) • Provides training to Community Workers and Contractors related to SRAMP, through the Security Advisor to the PIU • Seek WB no objections on SRAMP • Ensure the integration of local SRAMP requirements and adequate budgeting of security measures into bidding processes during procurement of Contractors • Monitor the implementation of SRAMPs by Social Safeguards in the regions/districts, and Contractors • Report on the implementation of SRAMPs as part of the reporting on environmental and social standards • Contribute to the development of local SRAMPs • Integrate SRAMP considerations into subproject design • Integrate SRAMP requirements into the subproject bidding documents • Contribute to decision making on implementation sites under due considerations of security risks.	• Present appropriate budget for security risk mitigation • Implement security risk mitigation measures for activity • Exercise right to suspend activities due to security threats • Act in accordance with social and environmental framework directives • Ensure all accidents, incidents and near misses are reported to the PIU immediately.

5.3 Security Management Measures

5.3.1 Overview

The following section outlines measures to mitigate the threats for the activities as assessed. Each threat category is presented with a risk level and accompanying mitigation measures for the project partners to implement. The threat scenarios are divided into four categories;

1. Threat to work sites.
2. Threat to movement.
3. Threat to local population.
4. Threat to staff

5.3.2 Worksite Security Measures

These measures apply to worksites being constructed under the project Components 1 and 2.

Table 5-2: Worksite Security Measures

Threat Category	Proposed mitigation measures
Political	• PIU to ensure continued alignment over the project. • Monitoring of political situation and potential developments. • PIU to ensure Region and District Administrations are aware of project and support it. • Potential risk to be managed in accordance with the project level Stakeholder Engagement Plan
Cultural	• Prior to starting work in a community; ▪ Project staff and project partners should commence initial familiarization and kick-off activities beginning with the local authority, sub clan leaders etc. ▪ Project staff and project partners should avoid all behaviours and practices that is not acceptable by the local communities – dressing, sub clan conflict topics/issue discussion, show off or superiority acts etc. ▪ Through project communication unit, transparent and clear project information in local language should be shared with the community ▪ Community of security practice members to work closely with both project staff and partner's staff. ▪ Ensure awareness of Grievance Redress Mechanism, including GBV channels. ▪ Create and employ effective community project participation measures including ensuring community involvement, community ownership and input. • Project activities are conducted by partners from the local area, where feasible, or the GSL at least, and project workers are representative and inclusive of local members to avoid any potential conflict. • Project personnel are trained to avoid and de-escalate any disagreements related to clan, politics or other potentially emotive concepts. Where complaints against the project exist, these will be referred to the Grievance Redress Mechanism. • Ensure District Commissioners and key officials in the location are aware of Project and its importance, mainly how it will assist local communities, and ensure they can support or intervene to de-escalate tensions. Such communications and discussions are to be managed in accordance with the Stakeholder Engagement Plan.
Safety	**Worker Safety** • Prior to construction a contractor must create a site specific Environmental Social Management Plan (C-ESMP). • Statements of works should also outline safety measures to be implemented at construction sites. • Contractors must ensure that they fully implement the preventative measures. • Safety monitoring must be conducted on a daily basis to identify the root causes of incidents (including near misses) and to understand how to prevent recurrences. • Prior to activity commencing engineers must conduct a visual inspection of the site to observe for general safety hazards. • Support from the security forces should be sought to conduct an inspection for any Unexploded Ordnance (UXO) hazards. **Site Hazards** Electrical Safety – a contractor should ensure that sites have an electrical safety plan. This plan should ensure inspection of electrical cabling;

	identification of electrical wiring at site; a lock out/tag out procedure to ensure that there is minimal risk of electrocution. • Noise – contractors should ensure workers are provided with hearing protection to prevent site noises impacting their hearing. Workers exposed to more than 85dB(A) should be provided with protection. • Welding – when welding or other hot works are conducted, the contractor will ensure that appropriate safety measures are in place. These will include eye protection and the set-up of a safety cordon. • Construction Waste–waste created from construction works should be disposed of in a safe manner. This may mean that a contractor must remove all waste from site and dispose of it in bulk in an approved manner. o Waste Incident Response Plan – there maybe occasions where construction waste spills into the natural environment, this may include debris but could also include harmful chemicals. The contractor should have in place a plan to address such spills that includes cleaning hazardous materials and rectifying any environmental damage. **Traffic Management** • Prior to commencing works the roads movement will use must be assessed for suitability. • The roads surrounding destination worksites must be reviewed and monitored to understand current road usage patterns. This information is to be used to develop a road safety assessment which identifies how additional traffic linked to project will impact local areas. • The road safety assessment and construction plan should be used by a contractor to develop a traffic management plan which deconflicts movement of vehicles and assets to worksites with the existing local conditions.
Criminal Activity	**Planning and Preparation** • Site set-up to ensure unused assets are stored securely. Such a storage area should have limited access points, for example no windows and a lockable door. The key will be held by the onsite security personnel and a log of who uses the key should be maintained. • Ensure there is adequate lighting within the site • Develop a clear procedure on asset movement from the one place to another to avoid loss or misplacement. • Write contingency plan covering criminal attacks such as armed robbery, kidnapping, GBV including rape and extortion. • Prepare site evacuation plan and keep updated. • Medical Response Plan must be in place. **External Support** • Communication with local stakeholders should be carried out in accordance with the project level Stakeholder Engagement Plan. • Contractor to liaise with local security forces and obtain up to date security briefings on the threat of criminal attacks on work sites. • Request increased patrols from local security forces in the area of the work site through the local authority which has a responsibility to provide a safe operating environment for project delivery. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operational Controls** • Random perimeter patrols to deter entry. • Conduct vetting/background checks of employees. • Minimize on site cash holdings. o Local security forces to provide personnel to conduct random perimeter patrols to deter unauthorised entry. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are

	made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU)-monitor violent incidents and trends in the area of the site. • Conduct regular staff security awareness briefings. Personnel to be briefed on security controls, critical incident response measures and site safety. • Conduct regular contingency plan rehearsals (where possible involve local security forces).
Extremist	**Planning and Preparation** • Site set-up to provide safe haven for personnel in case of attack, for example, no windows, a lockable door and blast protection. • Where possible there should be adequate standoff between working areas and roads • Write contingency plan covering extremist attacks such as direct fire, indirect fire, IEDs, kidnapping and extortion. • Access control policy and procedures. • Site evacuation procedures and plan. • Medical Response Plan must be in place. • Provide on-site trauma medical packs. **External Support** • Communication with local stakeholders should be carried out in accordance with the project level Stakeholder Engagement Plan. • Contractor to liaise with local security forces and obtain up to date security briefings on the threat of extremist attacks on work sites – must react to increased threat levels and limit movement of staff along routes and inform the respective PIU and if this curtails project activity. • Request increased patrols from local security forces in the area of the work site through the local authority which has a responsibility to provide a safe operating environment for project delivery. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operational Controls** • Issue Project ID cards to all site workers and staff. • Local security forces to provide personnel to conduct site security including; o Visual Search of vehicles at entrance to site using under vehicle search mirrors in purpose-built blast protection search bay. o Pat-down and metal detection wand search of vehicle driver and passengers prior to entry to facility. o Random perimeter patrols to deter unauthorised entry. • Visitors' vehicles to be parked 50metres distant from facility perimeter. • Use of Siren/Air Horn warning signals to alert facility personnel to shelter in refuge. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Conduct regular staff security awareness briefings. Personnel to be briefed on security controls, critical incident response measures and site safety. Conduct

	regular contingency plan rehearsals (where possible involve local security forces).
Communal Violence	**Planning and Preparation** • Site set-up to provide safe haven for personnel in case of attack, for example, no windows, a lockable door and blast protection. • Where possible there should be adequate standoff between working areas and roads • Write contingency plan covering extremist attacks such as direct fire, indirect fire, kidnapping, GBV and extortion. • Access control policy and procedures. • Site evacuation procedures and plan. • Medical Response Plan must be in place. • Provide on-site trauma medical packs. • Any project personnel being sent to an area should be vetted to ensure there are no pre-existing communal tensions between the personnel's clan and clan groups in area. o Vetting information to be supplied by staff member to PIU Security Advisor. o If vetting identifies potential for communal violence either alternate personnel should be identified OR local authorities and communal elders approached to gain assurances for the person's safety while in the area. **External Support** • Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Contractor - consult with local population and seek input. If population indicate that project activity is resulting in increased communal tensions stop project activity! – inform local security forces and PIU. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Request increased patrols from local security forces in the area of the work site through the local authority which has a responsibility to provide a safe operating environment for project delivery. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operational Controls** • Conduct vetting / background checks of employees. • Issue Project ID cards to all site workers and staff. • Local security forces to provide personnel to conduct site security including; o Visual Search of vehicles at entrance to site using under vehicle search mirrors in purpose-built blast protection search bay. o Pat-down and metal detection wand search of vehicle driver and passengers prior to entry to facility. o Random perimeter patrols to deter unauthorized entry. Visitors' vehicles to be parked 50 metres distant from facility perimeter. • Use of Siren/Air Horn warning signals to alert facility personnel to shelter in refuge. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in

	the area of the site. • Conduct regular staff security awareness briefings. Personnel to be briefed on security controls, critical incident response measures and site safety. • Conduct regular contingency plan rehearsals (where possible involve local security forces).
Vested Interests	**Planning and Preparation** • Site set-up to provide safe haven for personnel in case of attack, for example, no windows, a lockable door and blast protection. • Where possible there should be adequate standoff between working areas and roads • Write contingency plan covering extremist attacks such as direct fire, indirect fire, kidnapping and extortion. • Access control policy and procedures. • Site evacuation procedures and plan. • Medical Response Plan must be in place. • Provide on-site trauma medical packs. **External Support** • Communication with local stakeholders should be carried out in accordance with the project level Stakeholder Engagement Plan. • Contractor-consult with local population and seek input. If population indicate that project activity is resulting in increased communal tensions stop project activity! – inform local security forces and PIU. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Request increased patrols from local security forces in the area of the work site through the local authority which has a responsibility to provide a safe operating environment for project delivery. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operational Controls** • Conduct vetting / background checks of employees. • Issue Project ID cards to all site workers and staff. • Local security forces to provide personnel to conduct site security including; ▪ Visual Search of vehicles at entrance to site using under vehicle search mirrors in purpose-built blast protection search bay. ▪ Pat-down and metal detection wand search of vehicle driver and passengers prior to entry to facility. ▪ Random perimeter patrols to deter unauthorised entry. • Visitors' vehicles to be parked 50 metres distant from facility perimeter. • Use of Siren/Air Horn warning signals to alert facility personnel to shelter in refuge. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Conduct regular staff security awareness briefings. Personnel to be briefed on security controls, critical incident response measures and site safety. • Conduct regular contingency plan rehearsals (where possible involve local security forces).
Security Operations	**Planning and Preparation** • Site set-up to provide safe haven for personnel in case of attack, for example,

	no windows, a lockable door and blast protection. • Where possible there should be adequate standoff between working areas and roads • Write contingency plan covering extremist attacks such as direct fire, indirect fire, kidnapping and extortion. • Access control policy and procedures. • Site evacuation procedures and plan. • Medical Response Plan must be in place. • Provide on-site trauma medical packs. **External Support** • Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Contractor - consult with local population and seek input. If population indicate that project activity is resulting in increased communal tensions stop project activity! – inform local security forces and PIU. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Ensure communication with the security forces and local authority to avoid any conflicts. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Conduct regular staff security awareness briefings. Personnel to be briefed on security controls, critical incident response measures and site safety. • Conduct regular contingency plan rehearsals (where possible involve local security forces).

5.3.3 Staff Security Measures

These measures are applicable to the selection of PIU offices, hotels and venues for meetings primarily under the project Components 1 and 2.

Table 5-3: Mobile Security Measures

Threat Category	Proposed Mitigation Measures
Political	• PIU to ensure continued alignment over the project. • Monitoring of political situation and potential developments. • State PIU to ensure Region and District Administrations along route of travel are aware of project and support it. • Potential risk to be managed in accordance with the project level Stakeholder Engagement Plan and SRAMP.
Cultural	• Project activities are conducted by partners from the local area, where feasible, or the GSL at least, and project workers are representative and inclusive of local members to avoid any potential conflict. • Project personnel are trained to avoid and de-escalate any disagreements related to clan, politics or other potentially emotive concepts. Where complaints against the project exist, these will be referred to the Grievance Redress Mechanism. • Ensure District Commissioners and key officials in the location are aware of the Project and its importance, mainly how it will assist local communities, and ensure they can support or intervene to de-escalate tensions. Such communications and discussions are to be managed in accordance with the project level Stakeholder Engagement Plan. • Potential risk to be managed in accordance with the Stakeholder Engagement

	Plan
Safety	• Planning and Preparation • Medical Response Plan must be in place. • Intra-community vehicle moves may use a single vehicle. • Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist. • Prior to commencing works the roads movement will use must be assessed for suitability. • Transport including movement of workers will be done under some sort of security surveillance to ensure safe transport. • The roads surrounding destination worksites must be reviewed and monitored to understand current road usage patterns. This information is to be used to develop a road safety assessment which identifies how additional traffic linked to the Project will impact local areas. • The road safety assessment and construction plan should be used by a contractor to develop a traffic management plan which deconflicts movement • of vehicles and assets to worksites with the existing local conditions.
Criminal	Personnel are to return fire (as limited by their RoE/RUF) to allow vehicles carrying project personnel to escape • During movement if vehicles are halted by checkpoints. o Identify who the controlling entity is and their demands. o If checkpoint is operated by formal or informal security actor and will not allow passage or personnel are demanding a fee to allow passage; ▪ Vehicles should halt movement. ▪ The situation should be assessed for risk. ▪ If assessed as safe to do so the respective SFP should be informed immediately and asked for support/ to address with the checkpoint commander/ ▪ If assessed that informing SFP while at checkpoint would endanger lives, vehicles should return to nearest safe haven/ start point and respective SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement. o If checkpoint is operated by criminal or extremist actors and will not allow passage or personnel are demanding a fee to allow passage; ▪ Vehicles should halt movement. ▪ The situation should be assessed for risk. ▪ If possible and does not endanger lives vehicles should return to nearest safe haven/ start point and SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement. ▪ If aborting movement is not possible (checkpoint controlling entity will not allow vehicles to return) the SFP should be informed immediately to facilitate negotiations for release. • At checkpoints, vehicles should stop and negotiations held with controlling entity to allow passage. If necessary, the SFP should be informed if vehicles are not allowed to pass a checkpoint. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site.

	• Regular security awareness briefings for staff and contractors to include hijack actions on drills.
	• Ensure staff and contractors to practice preventative measures including;
	  o Not carrying/displaying valuables (phones, laptops, jewelry, money, equipment etc);
	  o Careful selection of low-profile vehicles;
	  o Carrying ID cards;
	  o Ensuring project information is not shared outside appropriate channels.
	• Conduct bi-annual simulated incident response exercises to familiarise management and validate plan.
	• Conduct hostile awareness for all staff and contractors.

Extremist	**Planning and Preparation**
	• Write contingency plan covering extremist attacks such as direct fire, indirect fire, IEDs and kidnapping.
	• Medical Response Plan must be in place.
	• All movements must be approved by PIU Security Focal Point prior to be conducted.
	• A movement plan must be submitted for approval and sign-off 48 to 72 hours prior to scheduled movement departure.
	• PIU Security focal point to liaise with local authority and security forces and to postpone movement in the event of ongoing conflict along planned route.
	• Movement plans to detail;
	  o Team Selection – team members selected for the activity should be identified along with potential risk factors including;
	  ▪ Gender.
	  ▪ Age.
	  ▪ Clan group.
	  ▪ Political affiliations.
	  ▪ Identified family history/ relatives.
	  o Route – Routes should be planned ahead of time with alternate routes and safe-havens identified.
	  o Vehicles – list number and type of vehicles to be used.
	  ▪ Intra-community moves may use a single vehicle.
	  ▪ Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist.
	  ▪ Movement plan to detail vehicles intended for use on the movement to ensure suitability for the movement.
	  o Communications–Ensure workable communications with PIU, District Officials and Security Forces (HF/VHF Radio, Satellite Phone, Mobile Phone). Also, ensure contact details of key contacts are stored.
	  o Security Risk Situation – any risks likely to be encountered on the route to be conducted by the person requesting movement. Prior to approval, the person approving the request will verify the situation with security stakeholders (officials at the destination, security forces, etc.).
	  o Security provider – whether from a private security provider or state security forces. The level of security provided must be commensurate with the security risk situation.
	
	External Support
	• Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan.
	• Contractor to liaise with local security forces and obtain up to date security briefings on the threat of criminal activity on regularly used routes – must react to increased threat levels and limit movement of staff along routes and inform

	the respective PIU if this curtails project activity. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operational Controls** • Vehicle Movements; o Intra-community moves may use a single vehicle. o Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist. • Movement timings and routes to be varied and avoid setting patterns! Utilise staggered start times and finish times. • Maintain low profile moves – no uniforms or marked vehicles • When moving large pieces of equipment obtain security forces escort • Movement information and schedules to be handled in a secure manner to prevent information leakage to hostile actors. • No night moves unless authorised by project security in extreme emergency. • During movement if vehicles are attacked an assessment must be made as to the threat. o If possible and there are no roadblocks vehicles should attempt to drive through ambush attack site. o If the road is blocked and no forward movement is possible, vehicles should halt, personnel should extract from vehicles and seek cover. o Where vehicle movement is escorted by armed security personnel (from security forces or commercial security provider) armed personnel are to return fire (as limited by their RoE/RUF) to allow vehicles carrying project personnel to escape • During movement if vehicles are halted by checkpoints. o Identify who the controlling entity is and their demands. o If checkpoint is operated by formal or informal security actor and will not allow passage or personnel are demanding a fee to allow passage; ▪ Vehicles should halt movement. ▪ The situation should be assessed for risk. ▪ If assessed as safe to do so the SFP should be informed immediately and asked for support/ to address with the checkpoint commander ▪ If assessed that informing SFP while at checkpoint would endanger lives, vehicles should return to nearest safe haven/ SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement. o If checkpoint is operated by criminal or extremist actors and will not allow passage or personnel are demanding a fee to allow passage; ▪ Vehicles should halt movement. ▪ The situation should be assessed for risk. ▪ If possible and does not endanger lives vehicles should return to nearest safe haven/ start point and PIU SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement. ▪ If aborting movement is not possible (checkpoint controlling entity will not allow vehicles to return) the SFP should be informed immediately to facilitate negotiations for release. • Use of a covert advance vehicle to detect obstacle causing vehicle to reduce speed, suspicious objects on road or roadside, and reporting by radio to main convoy. • Vehicles must be guarded at all times when parked outside of secure area.

	• Parked vehicles must be visually checked for the attachment of an IED prior to movement. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Regular security awareness briefings for staff and contractors to include Hijack actions on drills. • Ensure staff and contractors to practice preventative measures including; o Not carrying/ displaying valuables (phones, laptops, jewelry, money, equipment etc); o Careful selection of low-profile vehicles; o Carrying ID cards; o Ensuring project information is not shared outside appropriate channels. • Write and practice contingency plan covering criminal attacks such as armed robbery, kidnapping and extortion. • Conduct bi-annual simulated incident response exercises to familiarise management and validate plan. • Conduct hostile awareness training for all staff and contractors.
Communal Violence	**Planning and Preparation** • Write contingency plan covering violent attacks such as direct fire, indirect fire, kidnapping and extortion. • Medical Response Plan must be in place. • All movements must be approved by PIU Security Focal Point prior to be conducted. • A movement plan must be submitted for approval and sign-off 48 to 72 hours prior to scheduled movement departure. • PIU Security focal point to liaise with local authority and security forces and to postpone movement in the event of ongoing conflict along planned route. • Movement plans to detail; o Team Selection – team members selected for the activity should be identified along with potential risk factors including; ▪ Gender. ▪ Age. ▪ Clan group. ▪ Political affiliations. ▪ Identified family history/ relatives. o Route – Routes should be planned ahead of time with alternate routes and safe-havens identified. o Vehicles – list number and type of vehicles to be used. ▪ Intra-community moves may use a single vehicle. ▪ Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist. ▪ Movement plan to detail vehicles intended for use on the movement to ensure suitability for the movement. o Communications–Ensure workable communications with PIU, District Officials and Security Forces (HF/VHF Radio, Satellite Phone, Mobile Phone). Also, ensure contact details of key contacts are stored. o Security Risk Situation – any risks likely to be encountered on the route to be conducted by the person requesting movement. Prior to approval, the person approving the request will verify the situation with security stakeholders (officials at the destination, security

forces, etc.).
    - Security provider – whether from a private security provider or state security force. The level of security provided must be commensurate with the security risk situation.

External Support

- Contractor to liaise with local security forces and obtain up to date security briefings on the threat of criminal activity on regularly used routes – must react to increased threat levels and limit movement of staff along routes and inform the PIU if this curtails project activity,

Operational Controls

- Vehicle Movements;
    - Intra-community moves may use a single vehicle.
    - Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist.
- Movement timings and routes to be varied and avoid setting patterns! Utilise staggered start times and finish times.
- Maintain low profile moves – no uniforms or marked vehicles
- When moving large pieces of equipment obtain security forces escort
- Movement information and schedules to be handled in a secure manner to prevent information leakage to hostile actors.
- No night moves unless authorised by project security in extreme emergency.
- During movement if vehicles are attacked an assessment must be made as to the threat.
    - If possible and there are no roadblocks vehicles should attempt to drive through ambush attack site.
    - If the road is blocked and no forward movement is possible, vehicles should halt, personnel should extract from vehicles and seek cover.
    - Where vehicle movement is escorted by armed security personnel (from security forces or commercial security provider) armed personnel are to return fire (as limited by their RoE/RUF) to allow vehicles carrying project personnel to escape
- During movement if vehicles are halted by checkpoints.
    - Identify who the controlling entity is and their demands.
    - If checkpoint is operated by formal or informal security actor and will not allow passage or personnel are demanding a fee to allow passage;
        - Vehicles should halt movement.
        - The situation should be assessed for risk.
        - If assessed as safe to do so the SFP should be informed immediately and asked for support/ to address with the checkpoint commander/
        - If assessed that informing SFP while at checkpoint would endanger lives, vehicles should return to nearest haven/SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement.
    - If checkpoint is operated by criminal or extremist actors and will not allow passage or personnel are demanding a fee to allow passage;
        - Vehicles should halt movement.
        - The situation should be assessed for risk.
        - If possible and does not endanger lives vehicles should return to nearest safe haven/ start point and respective State SFP be informed of situation, with movement to resume only when SFP has cleared movement OR security forces can escort movement.
        - If aborting movement is not possible (checkpoint

	controlling entity will not allow vehicles to return) the SFP should be informed immediately to facilitate negotiations for release. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Regular security awareness briefings for staff and contractors to include Hijack actions on drills. • Ensure staff and contractors to practice preventative measures including; o Not carrying/ displaying valuables (phones, laptops, jewelry, money, equipment etc.); o Careful selection of low-profile vehicles; o Carrying ID cards; o Ensuring project information is not shared outside appropriate channels. • Conduct bi-annual simulated incident response exercises to familiarise management and validate plan. • Conduct hostile awareness training for all staff and contractors. • Medical Response Plan must be in place.
Vested Interests	**Planning and Preparation** • Consult with local officials and population and seek input. If population indicate that project activity is resulting in increased economic tensions that may lead to clashes in the area stop project activity! – inform local security forces and PIU. Communications and consultation to be conducted in accordance with Stakeholder Engagement Plan. • Write contingency plan covering violent attacks such as direct fire, indirect fire, kidnapping and extortion. • Medical Response Plan must be in place. • All movements must be approved by PIU Security Focal Point prior to be conducted. • A movement plan must be submitted for approval and sign-off 48 to 72 hours prior to scheduled movement departure. • PIU Security focal point to liaise with local authority and security forces and to postpone movement in the event of ongoing conflict along planned route. • Movement plans to detail; o Team Selection – team members selected for the activity should be identified along with potential risk factors including; ▪ Gender. ▪ Age. ▪ Clan group. ▪ Political affiliations. ▪ Identified family history/ relatives. o Route – Routes should be planned ahead of time with alternate routes and safe-havens identified. o Vehicles – list number and type of vehicles to be used. ▪ Intra-community moves may use a single vehicle. ▪ Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist. ▪ Movement plan to detail vehicles intended for use on the movement to ensure suitability for the movement.

	○ Communications – Ensure workable communications with PIU, District Officials and Security Forces (HF/VHF Radio, Satellite Phone, Mobile Phone). Also, ensure contact details of key contacts are stored. ○ Security Risk Situation – any risks likely to be encountered on the route to be conducted by the person requesting movement. Prior to approval, the person approving the request will verify the situation with security stakeholders (officials at the destination, security forces, etc.). ○ Security provider – whether from a private security provider or state security force. The level of security provided must be commensurate with the security risk situation. **External Support** • Contractor to liaise with local security forces and obtain up to date security briefings on the threat of criminal activity on regularly used routes – must react to increased threat levels and limit movement of staff along routes and inform the PIU if this curtails project activity, **Operational Controls** • Vehicle Movements; ○ Intra-community moves may use a single vehicle. ○ Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist. • Movement timings and routes to be varied and avoid setting patterns! Utilise staggered start times and finish times. • Maintain low profile moves – no uniforms or marked vehicles • When moving large pieces of equipment obtain security forces escort • Movement information and schedules to be handled in a secure manner to prevent information leakage to hostile actors. • No night moves unless authorised by project security in extreme emergency. ▪ If attacked vehicles should attempt to drive through ambush attack site. If road blocked, try to reverse out. If road blocked front and rear extract from vehicles and seek cover. ▪ If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Regular security awareness briefings for staff and contractors to include Hijack actions on drills. • Ensure staff and contractors to practice preventative measures including; ○ Not carrying/ displaying valuables (phones, laptops, jewelry, money, equipment etc.); ○ Careful selection of low-profile vehicles; ○ Carrying ID cards; ○ Ensuring project information is not shared outside appropriate channels. • Conduct bi-annual simulated incident response exercises to familiarise management and validate plan. • Conduct Hostile Awareness training for all staff and contractors. ○ Medical Response Plan must be in place.
Security Operations	**Planning and Preparation**

	• Write contingency plan covering violent attacks such as direct fire, indirect fire, kidnapping and extortion. • Medical Response Plan must be in place. • All movements must be approved by PIU Security Focal Point prior to be conducted. • A movement plan must be submitted for approval and sign-off 48 to 72 hours prior to scheduled movement departure. • PIU Security focal point to liaise with local authority and security forces and to postpone movement in the event of ongoing conflict along planned route. • Movement plans to detail; o Team Selection – team members selected for the activity should be identified along with potential risk factors including; ▪ Gender. ▪ Age. ▪ Clan group. ▪ Political affiliations. ▪ Identified family history/ relatives. o Route – Routes should be planned ahead of time with alternate routes and safe-havens identified. o Vehicles – list number and type of vehicles to be used. ▪ Intra-community moves may use a single vehicle. ▪ Inter-community vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled and to ensure if a vehicle accident occurs there are colleagues onsite to assist ▪ Movement plan to detail vehicles intended for use on the movement to ensure suitability for the movement. o Communications – Ensure workable communications with PIU, District Officials and Security Forces (HF/VHF Radio, Satellite Phone, Mobile Phone). Also, ensure contact details of key contacts are stored. o Security Risk Situation – any risks likely to be encountered on the route to be conducted by the person requesting movement. Prior to approval, the person approving the request will verify the situation with security stakeholders (officials at the destination, security forces, etc.). o Security provider – whether from a private security provider or state security force. The level of security provided must be commensurate with the security risk situation. **External Support** • Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Contractor to liaise with local security forces and obtain up to date security briefings on the threat of criminal activity on regularly used routes – must react to increased threat levels and limit movement of staff along routes and inform the PIU if this curtails project activity. • Ensure workable communications with local security forces (HF/VHF Radio, Satellite Phone, Mobile Phone). **Operation Controls** • All vehicle moves should be two plus vehicles to allow for cross-boarding in the event a vehicle is disabled. • Movement timings and routes to be varied and avoid setting patterns! Utilise staggered start times and finish times. • Maintain low profile moves – no uniforms or marked vehicles • When moving large pieces of equipment obtain security forces escort

	• Movement information and schedules to be handled in a secure manner to prevent information leakage to hostile actors. • No night moves unless authorised by project security in extreme emergency. • If attacked vehicles should attempt to drive through ambush attack site. If road blocked, try to reverse out. If road blocked front and rear extract from vehicles and seek cover. Use of a covert advance vehicle to detect obstacle causing vehicle to reduce speed, suspicious objects on road or roadside, and reporting by radio to main convoy. • Vehicles must be guarded at all times when parked outside of secure area. • Parked vehicles must be visually checked for the attachment of an IED prior to movement. • If security personnel from commercial providers are used, these must be appropriately managed and overseen by the contractor. Where complaints are made against armed guards these must be addressed using the Grievance Redress Mechanism. Guidance on the use of security personnel is provided in the Supporting Security Procedures section. **Awareness** • Contractor (with support from PIU) - monitor violent incidents and trends in the area of the site. • Regular security awareness briefings for staff and contractors to include Hijack actions on drills. • Ensure staff and contractors to practice preventative measures including; o Not carrying/ displaying valuables (phones, laptops, jewelry, money, equipment etc); o Careful selection of low-profile vehicles; o Carrying ID cards; o Ensuring project information is not shared outside appropriate channels. • Write and practice contingency plan covering criminal attacks such as armed robbery, kidnapping and extortion. • Conduct bi-annual simulated incident response exercises to familiarise management and validate plan. • Conduct hostile awareness training for all staff and contractors.

5.3.4 Community Security Measures

These measures apply to ensure the safety of communities in close proximity to component 1 and 2 sites and the movement of staff and assets under all components passing through communities.

Table 5-4: Community Security Measures

Threat Category	Proposed Mitigation Measures
Political	• PIU to ensure continued alignment over the project. • Monitoring of political situation and potential developments. • PIU to ensure Region and District Administrations in areas surrounding worksites have no objections to project. • Potential risk to be managed in accordance with the project level Stakeholder Engagement Plan
Cultural	• Project activities are conducted by partners from the local area, where feasible, or the GSL at least, and project workers are representative and inclusive of local members to avoid any potential conflict. • Project personnel are trained to avoid and de-escalate any disagreements related to clan, politics or other potentially emotive concepts. Where complaints against the project exist, these will be referred to the Grievance Redress Mechanism. • Ensure District Commissioners and key officials in the location are aware of

	project and its importance, mainly how it will assist local communities, and ensure they can support or intervene to de-escalate tensions. Such communications and discussions are to be managed in accordance with the project level Stakeholder Engagement Plan.
Safety	• Prior to construction a contractor must create a site specific Environmental Social Management Plan (C-ESMP). • Statements of works should also outline safety measures to be implemented at construction sites. • Contractors must ensure that they fully implement the preventative measures. Engagement and Grievance Redress – communications with communities is critical and ongoing engagement is required by all contractors.
Criminal	• Criminal activity management policy and procedures. • Evaluate level of severity, credibility, and potential impact of activity. • Enhance physical security of personnel and sites if required. • Consider seeking assistance/advice from local enforcement. • Crisis management /Incident response plan. • Maintain strict security of information • Contractors should also maintain oversight of any security personnel deployed to secure a worksite to ensure that they do not pose a threat to local • communities.
Extremist	• Consult with local population and seek input. If population indicate that project activity is resulting in increased likelihood of extremist attack perpetrated directly against them stop project activity! – inform local security forces and PIU, maintain communication with local population and in consultation reengage with project works once situation has stabilised. • Seek local security forces presence throughout duration of project activity in local community • Utilise local clan leader and senior stakeholder connections to mitigate risk. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan.
Communal Violence	• Consult with local population and seek input. If population indicate that project activity is resulting in increased communal tensions stop project activity! – inform local security forces and PIU, maintain communication with local population and in consultation reengage with project works once situation has stabilised. • Seek local security forces presence throughout duration of project activity in local community • Utilise local clan leader and senior stakeholder connections to mitigate risk. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan.
Vested Interests	• Consult with local officials and population and seek input. If population indicate that project activity is resulting in increased economic tensions that may lead to clashes in the area stop project activity! – inform local security forces and PIU, maintain communication with local population and in consultation reengage with project works once situation has stabilised. • Seek local security forces presence throughout duration of project activity in local community • Communication with local stakeholders, including vested interest groups and communities should be carried out in accordance with the Stakeholder Engagement Plan.

5.3.5 Project Assets Security Measures

These measures apply to ensure the safeguarding of project assets/properties.

Table 5-5: Project Assets Security Measures

Threat Category	Proposed Mitigation Measures

Community Violence/Vandalism	• Seek local security forces presence throughout the duration of project activity in local community • Utilise local clan leader and senior stakeholder connections to mitigate risk. Communication with local stakeholders should be carried out in accordance with the Stakeholder Engagement Plan. • Consult with local officials and population and seek input. If population indicate that project activity is resulting in increased economic tensions that may lead to clashes in the area stop project activity! – inform local security forces and PIU, maintain communication with local population and in consultation reengage with project works once situation has stabilized • Perimeter Security: Install a sturdy fence with secure gates and access control systems like key cards or codes. • Lighting: Ensure the site is well-lit, especially around storage areas and entry points, to deter thieves. • Employee Training: Educate employees on security protocols, best practices for securing equipment, and how to report suspicious activity. • Vigilance: Encourage employees to be vigilant and report any unusual activity or potential threats. • Insurance: Obtain comprehensive contractors' equipment insurance to minimize financial losses in case of protests. • Security Plan: Develop and implement a comprehensive security plan that outlines procedures for preventing and responding to community violence.
Theft/Robbery	Implement a multi-layered approach including physical security measures, access control, surveillance, and asset tracking systems. Physical Security: ▪ Secure Storage: Store equipment and materials in locked, fenced areas with restricted access. ▪ Perimeter Security: Install a sturdy fence with secure gates and access control systems like key cards or codes. ▪ Lighting: Ensure the site is well-lit, especially around storage areas and entry points, to deter thieves. ▪ Material Storage: Store valuable materials securely, possibly inside buildings or locked containers. Surveillance and Access Control: ▪ CCTV Cameras: Deploy surveillance cameras with deterrent features like motion detection and floodlights. ▪ Access Control: Implement strict access control protocols, such as key cards or biometric systems, to limit entry to authorized personnel only. ▪ Regular Monitoring: Monitor surveillance footage and access logs to detect and respond to suspicious activity. Asset Tracking and Identification: ▪ Asset Tracking Systems: Utilize GPS tracking devices to monitor the location of equipment and materials, especially valuable items. ▪ Asset Tags: Use metal or barcode tags with unique identifiers to track and manage assets. ▪ Inventory Management: Maintain a detailed inventory of all assets, including serial numbers and photographs, to facilitate recovery in case of theft. Workforce Awareness and Training: ▪ Employee Training: Educate employees on security protocols, best practices for securing equipment, and how to report suspicious activity. ▪ Vigilance: Encourage employees to be vigilant and report any unusual activity or potential threats.

	Additional Measures: ■ Insurance: Obtain comprehensive contractors' equipment insurance to minimize financial losses in case of theft. ■ Security Plan: Develop and implement a comprehensive security plan that outlines procedures for preventing and responding to theft. ■ Deterrent Features: Use anti-theft decals or labels on equipment to make it less attractive to thieves.

5.3.6 SRAMP Adaptability

Security risk management and mitigation will be adaptive to the risk and circumstances and will change in response to risk levels. In instances where security issues escalate or de-escalate, the security risk assessment and any existing management plans will be adjusted, following discussion with the Bank. In case of such adjustments, a summary of material changes will also be communicated to local stakeholders, in accordance with stakeholder engagement and information disclosure requirements outlined in ESS10.

5.4 Supporting Security Procedures

5.4.1 Use of Armed Guards

While the security situation in the project area of focus may, depending on the results of a security risk assessment, necessitate the use of armed guards at worksites, the project must be mindful of the risks presented by untrained, ill-disciplined or ill-equipped security guards. Untrained or poorly trained security personnel may engage in conduct which negatively impacts project workers, project affected persons and/or project assets. Risks can include;

- Unauthorised discharge of weapons against project affected persons;
- Theft of project assets or property from communities where project activities are taking place;

Gender Based Violence (GBV) and Sexual Exploitation and Abuse (SEA) and sexual harassment targeting project workers or and project affected persons. The use of guards is, as outlined above, only to be done when a security risk assessment shows a clear need. Prior to contracting guards, or obtaining from the local authority, a contractor must first implement passive measures such as installing fencing, lights, barriers and providing appropriate training to project personnel. The use of guards at the project sites is, above all, governed by the principles outlined in the World Bank ESS4: Community Health and Safety.

The use must be;

- Proportional to the threat level;
- Follows Good International Industry Practice (GIIP)
- In accordance with applicable State and Federal law
- In defensive use only to prevent risk to the life of project personnel, project affected personnel and project assets.

Where feasible, guards will be requested from the local authorities, with the support of the PIU. Where guards are supplied from the authorities the measures outlined below should still be applied (although they will likely not implement the sample Code of Conduct in Annex C). However, where guards are provided by the local authority it is nonetheless

critical that the Rules of Engagement (RoE) these guards will operate under is obtained and submitted to the PIU for approval prior to their deployment to protect a site.

Where a local authority cannot provide guards, where guards supplied operate under a RoE that may place civilians at risk (or there is no documented RoE) or there are conduct issues observed following an audit, alternative guard suppliers, including commercial providers may be selected. Where a local commercial security provider is selected to supply guards, the contractor must ensure that the security provider is appropriately licensed and registered with the FGS and respective FMS administration and is approved by the respective local authority.

Where non-Somali staff (or dual nationality Somalialand personnel) are expected to travel to worksites contractors will be expected to contract a licensed private security provider that is able to supply B6 level armoured vehicles and appropriately licensed armed guards.

The use of Armed Guards can potentially increase some risks in that;

- Guards may react inappropriately to situations, posing a risk to others or themselves;
- Guards may fail to perform their duties adequately, allowing threat actors to target the project;
- Guards lead to situations of misconduct against the wider community or colleagues. The risks of using armed guards are to be addressed through four channels, outlined below.

Selection of Guards and Suppliers

Prior to being contracted to supply guards, a guard supplier should be screened by the PIU, supported by SRMC, to ensure that they meet expected standards.

The screening process will check;

- Licence and registration of the company and the weapons they are supplying;
- Management processes;
- Guard training syllabus;
- The company's existing Code of Conduct and Rules for the Use of Force;
- The backgrounds, where possible, of the guards proposed for the worksite and that they have not been involved in past abuses.

It is, unfortunately, expected that not all local suppliers will be able to meet these criteria. While elements such as licencing and registration cannot be ignored, if a company does not have a documented Guard Training syllabus, Code of Conduct or Rules for the Use of Force, standardised versions created by the SRMC on behalf of the PIU can be supplied, along with support for the supplier to operationalise these.

The intention of ensuring guard suppliers have existing Codes of Conduct, Rules for the Use of Force, Management processes, and training syllabus is to ensure a basic level of management control exists.

Sample Code of Conduct

Where a security provider does not have an existing Code of Conduct, or the Code of Conduct does not meet project requirements, they will be expected to comply with the sample Code included at Annex C.

Procedures
Guards working on project sites will be expected to follow the security measures specific to the site as outlined in this SRAMP. This includes measures such as Access Control, Patrolling, Incident Response, including the Code of Conduct and Rules for the Use of Force created for project. It is recommended that during the process to contract armed guards and deploy them to project sites the supplier is requested to provide their procedures for review and approval by the PIU Security Advisor, with support from the SRMC.

Training
While only guards that have received a basic level of training should be supplied to project sites, to meet the requirements of this SRAMP, additional training should be provided. This training will ensure that guards have been made familiar with the project controls relating to armed guards and their duties.

Monitoring Security Guards
During the deployment of security personnel, performance should be monitored throughout by the security provider to ensure professional and appropriate conduct. Any operation which may require the use of force should be closely supervised and monitored by management to ensure that the use of force, if required, is permissible and appropriate in the circumstances. The role of management monitoring the operation is to ensure that the operational plan is followed correctly, that all reasonable steps to avoid the use of force are taken by the deployed personnel, and that the use of force continuum is applied wherever required.

Supervision and monitoring also serve to reprimand and reorient the security personnel who might diverge from the operational plan, those who may be tempted to resort to the use of force when not necessary, or those who have been accused of misconduct. Throughout the operation, the responsibility of the management is to ensure the respect of the principles of necessity, proportionality and precaution and to adopt means and measures to ensure that those principles are upheld.

In cases where this fails, managers are responsible for ensuring accountability. Proper supervision and monitoring will play a crucial role after the operation, whenever an incident involving the use of force might require reporting, investigation or disciplinary sanctions. Failure to adequately supervise or monitor security personnel during an operation that involves or potentially requires the use of force might engage the responsibility and accountability of those in management positions.

Security providers (whether a commercial provider or from the security forces) should:

- Establish and maintain a clearly defined management structure. Responsibilities should be clearly defined, documented and communicated. Roles should include tasks such as monitoring, coordination and supervisory responsibilities, as well as planning, security, incident management, response and/or recovery. Roles should be paired with appropriate authority, adequate resources and rehearsed operational plans and procedures to effectively deal with disruptive and undesirable events;
- Establish communication procedures to share information about the security team activity, and its operational and logistical status, the relevant threat information and incident reporting to company management, clients, other private security teams and relevant authorities;

- Establish and implement procedures to support the protection of people, assets and other security related functions, including managing risks;
- Establish and implement procedures to 1) identify undesirable or disruptive events, 2) define how the security provider prevents, mitigates, and responds to undesirable or disruptive events, and 3) document how the security provider will proactively prevent, mitigate, and respond to such events.

Security grievance reporting mechanism

The SRAMP adopts the Project level grievance mechanism for security complaints, integrated with project and stakeholder engagement. Collaboration with security leaders aligns with internal procedures. Key steps include publicizing procedures, receiving, and tracking grievances, reviewing, and investigating, developing resolutions, and monitoring. Security personnel grievances should be addressed using alternate channels depending on the security supplier in question;

- Private security personnel – the project GRM process applies;
- Local Authority security personnel – the project GRM process applies, but complaints are to be passed to the State administration and local authority;
- Somali National Police – follow Somali National Police Force and Independent Policing Oversight Authority protocols for resolution
- Somali National Army – complaints should be escalated to the personnel's unit.

Key Steps in the security-related GRM process

Key Steps:

- Record the incident or allegation.
- Monitor and communicate outcomes.
- Take corrective action to avoid recurrence.
- Collect information promptly.
- Report any unlawful act
- Protect confidentiality.
- Document the process.
- Assess the allegation or incident.

Conduct further inquiry if warranted

The monitoring of security, and security suppliers, performance will be an ongoing process and should be driven by inputs from within the project PIU and the wider community. Project Personnel will have the right to report concerns over security and risks internally to their employer or PIU representative in accordance with the project GRM. These risks will be addressed within the GRM system with the SRMC able to provide advisory support and guidance as necessary.

Communities may follow a similar process for addressing security concerns and concerns regarding the performance of armed guards at a project site as per the project level SEP. Grievances against armed guards should be handled discretely with a view to preventing further misconduct. Where armed guards are to be investigated, they should be removed from the site as soon as the grievance is reported. Depending on the nature of the grievance, local security authorities may also need to be informed, particularly if the accusation relates to a serious crime.

Where an investigation demonstrates misconduct was the result of a lack of supervision and leadership by the relevant security supplier, the supplier should be removed from the site and a new supplier hired, or punitive clauses in contracts should be invoked. Project-affected persons (PAPs) may also make complaints directly to the project-wide GRM through the key contact persons (Grievance officer).

Security Procurement Process

All procurement/contracting of security providers or the purchase of security equipment should be conducted in accordance with; Section 6 Procurement of the project Operations Manual; and Section 6.6 of the Security Management Framework.

The key principles for procuring security services/supplies are;

1. All security suppliers must comply with, and implement, the relevant Security Management measures during delivery works;
2. Deploy armed personnel only when authorised;
3. Ensure they have a Code of Conduct that exceeds Annex C or implement a similar Code of Conduct;
4. Ensure they have Rules for the Use of Force that exceed Annex D or implement a similar approach to the use of force, that includes a graduated force response/ escalation of force mechanism;
5. Can demonstrate appropriate licencing and certification, including that weapon are properly licenced with Federal and State authorities;

Guidance on security obligations for contractors selected to deliver project activities are outlined in Annex B.

Security Community of Practice

To support the management of security and improvements in the security processes the PIU with the support of the SRMC will set up a security community of practice that provides a forum for the monitoring of security, exchange of ideas and provision of security awareness information. The community of practice will include stakeholders from across the project including, but not limited to;

PIU Security Advisor (who leads the community of practice);

- PIU security focal points;
- Local authority representatives;
- Contractor security focal points;
- Security officials from formal security providers (Somaliland Police Force, custodial corps, coastal guards, and the National Intelligence Agency (NIA).
- NGO and international organisations.

The community of practice will also provide an input into monitoring the performance of the security management system as detailed below.

Security Management Plan Monitoring

Overview

To ensure that the measures outlined in the SRAMP are implemented and continue to manage the risks to the project and affected communities, ongoing performance monitoring will be conducted across the project.

In keeping with ISO31000, the Security Risk Assessment process is an ongoing activity. During project delivery, the operational environment and implemented controls will be assessed, reviewed and if need be, updated in accordance with the methodology outlined in the Project Security Risk Assessment and Management Plan document. A summary of material changes would also be communicated to local stakeholders, in accordance with stakeholder engagement and information disclosure requirements outlined in ESS10.

The ongoing security risk assessment will utilise information from the context monitoring process, which looks externally to the project, and the performance monitoring process which looks internally.

Context Monitoring

To support the ongoing risk assessment, process the SRMC will collect information from a range of sources as outlined in Figure 5-1 and use these inputs to feed into the ongoing information collection requirements (Figure 5-2) which will support a detailed understanding of the context.

Figure 5-1: Information Sources

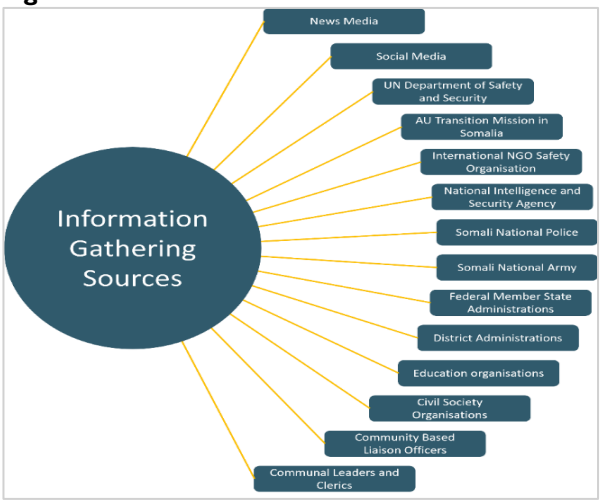
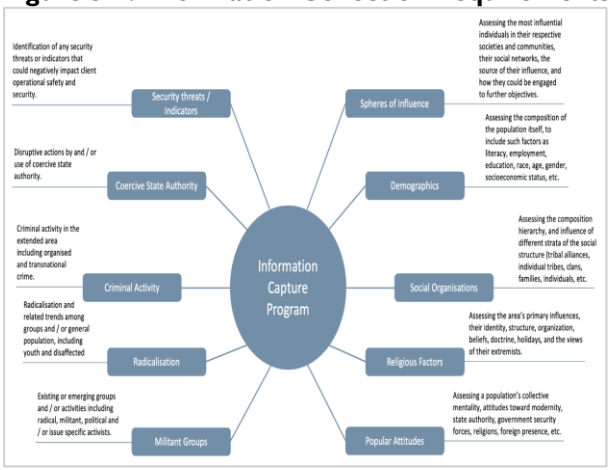


Figure 5-2: Information Collection Requirements



The collection of information as outlined in Figures 5-1 and 5-2 will permit ongoing updates of risk registers and support the implementation of appropriate security levels for a District.

Performance Monitoring

In addition to context monitoring during the project the performance of the SRAMP will also be monitored. Contractors will be expected, as part of their delivery to implement appropriate security measures to ensure the safety of project personnel, project affected communities and project assets. The goal of the performance monitoring process is to ensure that contractors are complying with these contractual requirements and that the measures undertaken are performing adequately.

Performance monitoring involves several elements;
Security Community of Practice–input from an extended community of practice as to the effectiveness of the security system will be sought. Contractor self-certification – contractors will be required to submit proof of SRAMP implementation at sites. They will be required to provide a copy of their Site or Activity Security Management Plan, contracts with private security providers (if applicable) and evidence where physical security measures are put in place (plans and photographs).

PIU/SRMC audit and inspection–the PIU (supported by the SRMC) will conduct site inspection activities during project delivery to provide verification that the contractor has properly implemented the measures outlined in the SRAMP and that the self-certification evidence provided is accurate.

Evaluation
The results of the ongoing monitoring activities will be reviewed and evaluated against the security management framework as well as the project's underlying principles, including the measures outlined in *Environmental and Social Standard 2: Labour and Working Conditions*, *Environmental and Social Standard 4: Community Health and Safety* and *Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel*.

By comparing the results of the monitoring with the evaluation framework, we will identify areas where the security management framework is either not working or can be improved. This information will then be used to improve the security management framework.

Reporting
The project will see several levels of reporting conducted. In addition to the documents created as part of the security management framework, namely the Project SRA and SMP, the District SRAs and SRAMPs and the Activity/Site SRAMPs, other documents will be created and shared with the PIU.

Incident reporting- as per the WB ESIRT, all ES incidents that have or result impact to the project personnel, workers, activities, communities, contractors and WB/MoEM reputation will be reported within 24 hours of their occurrence, typical or same WB ESIRT will be applied by the project. This tool will be confidential, owned and managed by the SA/SF while its utilization orientation/training will be conducted through the Bank's technical person/unit. WB will include the recipients of those incidents reported

GBV incidents reporting – all GBV incidents will be reported through specific GBV incident reporting tool that is managed by the GBV specialist and her GBV focal points at project activities sites/areas.

Risk Registers - will be created and hosted online and available for review at any time. These Risk Registers will combine the outcomes of the Security Risk Assessment and

Management Plans. The purpose of the Risk Registers will be to ensure that the PMU are able to track the overall Security and Safety Risk levels. They will be reviewed and updated following the monitoring and evaluation activities as outlined above. A summary of material changes would also be communicated to local stakeholders, in accordance with stakeholder engagement and information disclosure requirements outlined in ESS10.

Weekly Security Reports – these will provide updates to the PIU on the overall security and conflict context. Regular Security Community of Practice meetings on weekly/monthly basis. These meetings will include discussions on incidents and events, review system performance, assess changes to the Security Management Plan, identify new risks and lessons learnt.

Meetings will include;

a) PIU Security Advisor;
b) Monthly safeguarding team meetings;
c) Wider community of practice meetings on a monthly basis (or as called for by the PIU Security Advisor).

Incident Reports – in the event of an incident, we will work with key stakeholders to review and identify the incident, the root cause and lessons learnt and supply this to the PIU.

6 PROJECT CRITICAL INCIDENT MANAGEMENT FRAMEWORK

6.1 Overview

While the security and safety procedures detailed in the previous section are in place to reduce the likelihood of incidents occurring or ensure they are managed at the operational level, exceptional situations can arise that fall outside typical management arrangements due to their nature and severity. Successfully resolving and managing any critical incident depends on our ability to take appropriate decisions quickly, which requires preparation, a good flow of information, and clear channels of communication that all staff understand.

The objectives of Critical Incident Management are;

- **Prevent (further) harm and ensure the health and/or safety of the victim(s) and other personnel affected by the incident**–The first hours following (the onset of) a Critical Incident are often the most crucial, rendering instant reporting, a clear division of roles and responsibilities, and fast decision-making an absolute necessity;
- **Assure families of victims of a responsible and effective response** – Maintaining the confidence of victims' families is essential in establishing good relations and ensuring all stakeholders are "on board" during and after the incident;
- **Ensure continued organizational management and output during the incident** –Critical Incident Management is resource-intensive, especially for enduring incidents (for example, abductions). Planning and preparedness will mitigate the risk of the unnecessary distraction of senior management, thus contributing to the ability of the project to continue functioning**;**
- **Ensure project continuity**–In addition to mitigating the impact of a Critical Incident on organizational management, good Critical Incident preparedness contributes to our ability to continue project activities during a Critical Incident and/or restart operations in its aftermath;
- **Fulfil organizational responsibilities and reduce the risk of litigation/liability claims-**Contractual obligations and related litigation risks vary by country since we are subject to national legislation. We must ensure that we are fully aware of relevant legal labour frameworks, including those for national staff in each country of operation;
- **Safeguard organizational image and reputation**–Inadequate Critical Incident response, or perceived mishandling of a Critical Incident (in the eyes of media and/or family), can negatively affect the image of the project, with myriad consequences in countries of operation and at the international level (fundraising, recruitment, etc.). Again, a solid and professional Critical Incident response will help to mitigate this risk.

A small caveat, safeguarding reputation, while an important consideration, should never take precedence over the safety and well-being of staff, which remains the primary objective of Critical Incident Management within the project.

6.2 Critical Incident Management Team

The project has established a Critical Incident Management Team (CIMT) to respond to critical incidents. The CIMT has the following responsibilities. On receiving an incident report, the CIMT must decide the following;

- **Project Activities**-should these be suspended or personnel withdrawn to a more secure location;
- **Support-**should additional personnel be deployed to assist;
- **Information**-what should be circulated internally and externally, and any limitations or confidentiality issues.;
- **Objective**-how should the Critical Incident be resolved.

The CIMT is comprised of the following

- The PIU Coordinator
- PIU Project Security Advisor
- The PIU Environmental and Social Safeguards Specialists
- The respective State HR/procurement specialist (as relevant depending on FMS where the incident occurred);
- Project partner management, including those with safety and security responsibilities. The CIMT may also require the involvement (where requested by the CIMT) of
    - Key experts and officials from other Federal Ministries and Organisations (or State equivalents).

6.2.1 Critical Incident Management Procedures

Table 6-1: Critical Incident Management Procedures

Scenario	Project Team	Critical Incident Management Team
Relocation and evacuation	**Preventative** • Recommends evacuation to the Senior Management. • Will manage evacuation if authorized. **Emergency** • Alert CIMT of need to evacuate and how many personnel. • Identify how to evacuate and inform CIMT	**Preventative** • CIMT alerted and monitors to support if Project Team needs assistance. • Media Management **Emergency** • Assess the situation with personnel, partners and other stakeholders. • CIMT decides on evacuation. • CIMT to manage evacuation with input from Project Team. • Media Management
Medical response	• Provide 1st Aid and get to hospital. • Alert CIMT. • Support CIMT and Incident response.	• Implement Medical Incident Response Plan • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Provide Psychosocial support.
Injury of personnel	• Alert CIMT. • Support CIMT and Incident response.	• Implement Medical Incident Response Plan • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Media Management. • Provide Psychosocial support.

Death of personnel	• Alert CIMT. • Support CIMT and Incident response.	• Immediately notify Project Management Committee and Project Steering Committee. • Inform World Bank team. • Inform family/next of kin through family liaison. • Communicate with project personnel and other relevant parties. • Media Management. • Provide Psychosocial support.
Staff disappearance, Abduction, detention or kidnap	• Alert CIMT. • Continue to try and contact missing personnel. • Liaise with local partners to understand if Abduction/ Detention/Kidnap. • Support CIMT and Incident response.	• Immediately notify Project Management Committee and Project Steering Committee. • Inform World Bank team. • Implement Hostage Incident Management Plan. • Inform family/next of kin through family liaison. • Communicate with project personnel and other relevant parties. • Media management. • Provide Psychosocial support.
Attack or threat of attack against project activity (worksite/ movement)	• Alert CIMT. • Project activities to pause, personnel to shelter in place. • Liaise with authorities and other organisations working in the area	• Assess the situation with personnel, partners and other stakeholders. • Monitor situation and authorize pause or withdrawal of personnel if risk warrants it. • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Media management. • Provide Psychosocial support.
Attack on hotel where personnel are staying or at an office	• Alert CIMT and check how many personnel may be involved. • Try and contact personnel to check on status. • Liaise with local partners as necessary. • Liaise with authorities.	• Assess the situation with personnel, partners and other stakeholders. • Inform insurance. • Monitor situation and liaise with authorities. • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Media management. • Provide Psychosocial support.
Media or reputation crisis	• Do not respond. • Alert CIMT	• Do not respond until an assessment has been made and advice has been • sought from the media/comms team.

Disease outbreak/pandemic	• Alert CIMT and check how many personnel may be involved. • Liaise with local partners as necessary. • Liaise with authorities. • Provide PPE and support services to staff.	• Establish safety and wellbeing of personnel. • Restrict travel and activities to limit exposure. • Inform insurance • Ensure accurate information is passed to personnel. • Update health measures and contingency plans. • Work with Project Team to monitor health of personnel.

6.3 Violent Incident Response Plan

6.3.1 Overview

During project delivery, project personnel may be at risk of armed attack by criminals, communal militia and extremists. This section outlines how such incidents should be responded to. It should be noted, though, the below descriptions are to be seen as guidelines as opposed to an exact process as every situation is different and a document cannot account for all possible events. These procedures work in conjunction with the Critical Incident Management procedures in table above.

6.3.2 Direct Fire

If during project activities personnel come under direct fire (the firing of a ranged weapon whose projectile is launched directly at a target within the line-of-sight of the user) the following are steps that can be taken.

- Take cover–find closest hard cover and get behind it. Be wary of objects that provide concealment (hide from view) as opposed to cover (prevent projectiles striking).
- Return fire-if accompanied by armed security personnel (security forces or private security guards) these should fire on the person/s firing at the party, remembering the relevant Rules of Engagement (security forces) or Rules for the Use of Force (private security). Fire should be aimed and controlled and not towards civilians (to avoid inflicting casualties).
- Evacuate – leave area expeditiously towards a safe location. If with vehicles (and if undamaged) use these to evacuate area.
- Rally- all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- Report-inform local security forces, PIU and community stakeholders of the situation and what has happened.

Direct Fire Attack on Office/Hotel–Active Shooter Situation

There is potential that while the project personnel are in building (including Hotels or Offices) the site could come under attack by armed individuals (extremists, communal militia, criminals) who are able to enter, leading to an active shooter situation. The response is based on, but with differences, to the usual Direct Fire response plan due to differences in environment, availability of cover, restricted movement etc. The following are steps that can be taken.

- **Run** - If there is an accessible escape path, attempt to evacuate the premises. Be sure to:
    - Have an escape route and plan in mind

- Evacuate regardless of whether others agree to follow
- Leave your belongings behind
- Help others escape, if possible
- Prevent individuals from entering an area where the active shooter may be

- **Hide** – If evacuation is not possible, find a place to hide where the active shooter is less likely to find you. Your hiding place should:
  - Be out of the active shooter's view
  - Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
  - Not trap you or restrict your options for movement
  - To prevent an active shooter from entering your hiding place:
    - Lock the door
    - Blockade the door with heavy furniture
  - If the active shooter is nearby:
    - Lock the door
    - Silence your cell phone and/or pager
    - Turn off any source of noise (i.e., radios, televisions)
    - Hide behind large items (i.e., cabinets, desks)
    - Remain quiet
- **Fight** – As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:
  - Acting as aggressively as possible against him/her
  - Throwing items and improvising weapons
  - Yelling
  - Committing to your actions

Throughout the situation if members of the security forces arrive on scene ensure you cooperate with their instructions, remain calm and keep your hands visible.

6.3.3 Indirect Fire

- If during project activities personnel come under indirect fire (the firing of a ranged weapon without relying on a direct line of sight between the gun and its target) the following are steps that can be taken.
- Take cover – find closest overhead cover and get below it. If there is no overhead cover available personnel should assume the prone position.
- Evacuate – leave area expeditiously towards a safe location. If with vehicles (and if undamaged) use these to evacuate area.
- Rally – all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- Report – inform local security forces, PIU and community stakeholders of the situation and what has happened.

6.3.4 Explosive Hazards

During project activities personnel may observe or trigger an explosive hazard either an Improvised Explosive Device (IED) planted by extremists or Unexploded Ordnance (UXO) left from previous armed conflict. The following are steps that can be taken.

Observation of an IED/ UXO Threat

If a possible device IED/ UXO is observed and has not exploded.

- Alert – whoever sees the suspected device must raise the alarm. The alarm should use the 3Ds (Distance; Direction; Description).
- Stop – all movement within 200m of the suspected device must stop immediately.
- Evacuate – leave area expeditiously towards a safe location (at least 200m from the device).
- Rally – all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- Report – inform local security forces, PIU and community stakeholders of the situation and what has happened.

IED/ UXO Explosion

If an IED/ UXO explodes near project personnel.

- Stop – all movement within 200m of the suspected device must stop immediately.
- Evacuate – leave area expeditiously towards a safe location (at least 200m from the device).
- Rally – all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- Treat – Use the measures in the Medical Incident Response Plan.
- Report – inform local security forces, PIU and community stakeholders of the situation and what has happened.

6.4 Medical Incident Response Plan

6.4.1 General Requirements

- At least one employee at a worksite or in a convoy must have received emergency medical training (to FPOS-I or similar standard).
- A convoy or worksite must have sufficient medical equipment to address both day-to-day minor injuries, such as cuts and abrasions, expected in a construction project and more significant medical incidents such as gunshot or blast wounds resulting from attacks by threat actors. Project contractors must identify the nearest medical facility to a worksite capable of dealing with traumatic injuries and also identify the quickest, safest, route to reach this facility.
- Where no medical facility capable of dealing with traumatic injuries is within 30 minutes' drive of a worksite, a contractor should ensure they have provision to treat such injuries at a worksite, at least to the point of stabilizing an injured employee to the point where an evacuation to a more distant medical facility is feasible.

6.4.2 Medical Evacuation

Depending on the nature of injury project personnel may require a medical evacuation. There are three levels of medical evacuation considered within the project as outlined below.

Table 6-2: Medical Evacuation Procedures

Level	Scope	Reason	Requirements
1	Intra-District	• Traumatic injury that cannot be treated at worksite. • Traumatic injury that cannot be treated at nearby medical facility.	• Injured employee must be stabilised at scene for evacuation to be safe. • Contractor supplied vehicles to transport the injured party (ensuring movement security

			mitigations are employed)
2	Intra-Region or Intra-Somaliland	• Traumatic injury that cannot be treated at medical facility in District. • Persistent effects of an injury that require specialist care not available in District.	• Injured employee must be stabilised at local medical facility for evacuation to be safe. • Evacuation by road or air depending on medical condition of employee and prevailing security situation. • Movement by air requires properly supplied and configured aeromedical transport and flight medic.
3	International	• Persistent effects of an injury that require specialist care not available in Somaliland.	• Injured employee must be assessed as being stable enough for evacuation to be safe. • Evacuation by road or air depending on medical condition of employee and prevailing security situation. • Movement by air requires properly supplied and configured aeromedical transport and flight medic.

6.5 Hostage Incident Management Plan

6.5.1 Overview

During project delivery, project personnel may be at risk of kidnapping by criminals, communal militia and extremists. This section outlines how project partners should respond to such incidents. Kidnapping refers to forced capture and detention with the explicit purpose of obtaining something in return for the captive's release. The objective and hence the motive for kidnapping vary: often it is money, though kidnappers may also demand political concessions. In other cases, what may ostensibly be a political cause may in fact be little more than an extortion racket.

Table 6-3: Hostage Incident Management Plan

Stage	Activities
Prevention	• Operate according to procedures outlined in Section 1: Security Management Plan. • Ensure staff accountability and tracking systems are in place. • Conduct regular security and awareness briefings with personnel. • Avoid routine during movement. • Use protection where required by risk levels. • Establish a clear policy on payment of ransoms. • Training on basic self-defense techniques
Initial Response	• When personnel are reported missing, initially try and locate them. If unable to contact the person, then treat as if they are missing/ kidnapped; o Inform local security forces. o Halt all activities in District with personnel to shelter in place. o Limit spread of information. • Seek support of specialist advisors on kidnapping resolution
Managing the Incident	• Make contact with kidnapped personnel's families- face to face is best- and brief them. • Stand by to receive contact from kidnappers.

	• Nominate the communicator (and a backup) who will lead conversation with kidnappers. • Consider kidnapping scenarios and possible demands.
Communication with Kidnappers	• Response to kidnap will depend on group that conducted the kidnapping. • Criminal/ Communal kidnap (for ransom or grievance with clan/FGS). o CIMT (supported by Project Steering Committee and Project Management Committee) takes lead on all negotiations. o The communicator or back up to lead on conversations. o Communications to be kept calm, clear, professional. o Understand the kidnapper's demands. o Seek to establish Proof of Life as quickly as possible. o Maintain confidentiality and contain spread of information • Kidnap by extremist group. o CIMT (supported by Project Steering Committee and Project Management Committee) takes lead on all communications. o FGS policy is no negotiation with Khawarij. o CIMT (and supporting stakeholders) to use informal connections to speak to kidnappers, including using Clan connections to seek release. o The communicator or back up to lead on conversations. o Communications to be kept calm, clear, professional. o Understand the kidnapper's demands. o Seek to establish Proof of Life as quickly as possible. o Maintain confidentiality and contain spread of information
Media Management	• Try to minimize spread of information to reduce chances of leaks to media. • If media/social media report kidnaps a no comment response should be provided. • Media response is to be aligned with PIU, GSL and security forces.
Ending the Incident	• Kidnapping may take weeks to resolve. • Payment of ransoms is not encouraged but may be necessary. Should be aligned with all stakeholders (PIU, GSL, District Commission, security forces). • Abduction for political reasons may take longer to resolve. • When victim is released psychosocial support and counselling is an immediate need.

6.6 Region Incident Levels and Responses

During the course of the project, incidents that may affect the project or larger community are likely to occur. While incidents directly targeting project activities should be dealt with by procedures created by project partners operating in the region, incident levels elsewhere in the Region can escalate to the point where they pose a threat to the project, the personnel working on it and the wider community. During the course of project delivery, the situation in the project footprint should be monitored and appropriate measures, as outlined below be implemented.

Table 6-4: Region Incident Levels - Low Risk

Stage 1 Low Risk Level (Normal)			
• No overt political and cultural disputes in District relating to project or partners • No criminal activity or attacks by vested interests targeting project in previous 30 days • No extremist attacks in District • No communal violence in District affecting project in previous 30 days • Discussions with local communities do not indicate discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**

1	Low	Normal	• Business as usual • Weekly review of conditions • Quarterly review of staff contacts details, NOK, etc. • Review and rehearsal of procedures

Table 6-5: Region Incident Levels - Moderate Risk

Stage 2 Moderate Risk Level (Caution)			
• Increasingly overt political and cultural disputes in District relating to project or partners • No criminal activity or attacks by vested interests targeting project in previous 15 days • Limited extremist attacks in District with attacks occurring over 20Km of a worksite • No communal violence in District affecting project in previous 15 days • Discussions with local communities indicate low level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
2	Moderate	Caution	• Daily monitoring of conditions • Review incident response procedures • Review medical evacuation procedure • Review staff personal safety measures • Identity documents and go-bag contents to be carried by all individuals during all routine moves

Table 6-6: Region Incident Levels - High Risk

Stage 3 High Risk Level (Alert)			
• Increasingly overt political and cultural disputes in District and protests against project or partners • No criminal activity or attacks by vested interests targeting project in previous 7 days • Regular extremist attacks in District with attacks occurring over 5km of a worksite • Communal violence in District but is not within 5Km of a worksite • Discussions with local communities indicate increasing level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
3	High	Alert	• Daily monitoring of conditions • Consider pause of project activities and discuss with PIU • Be prepared to pause project at short notice • Prepare staff for evacuation at short notice

Table 6-7: Region Incident Levels - Extreme Risk

Stage 4 Extreme Risk Level (Emergency)			
• Overt political and cultural disputes in District with protests and armed attacks against project or partners • Criminal activity or attacks by vested interests target the project • Daily extremist attacks in District with attacks occurring within 5Km of a worksite OR extremist attacks on a project activity • Communal violence in District affecting project • Discussions with local communities indicate widespread level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
4	High	Emergency	• Project paused in District • Personnel to be evacuated or shelter in place • Project worksite to be secured

7 ANNEX

7.1 Annex A. Summary of Security Risks and Mitigation Measures

Table 7-1: Summary of Risks, Mitigations, Contingencies and Responsible Parties

Security Risk	Mitigation Measures	Contingency Plan	Responsible Party
Political	As listed in Tables	Contractor –Monitor as per Regional Incident Levels Contractor Level–Escalation to PIU/ CIMT PIU–Engage with relevant GSL authorities	Onsite–Contractor District – Local Authorities State – GSL Authorities Overall – PIU (security specialist) (with GSL support)
Cultural	As listed in Tables	Contractor – Monitor as per Regional Incident Levels Contractor Level –Escalation to PIU/ CIMT PIU–Engage with relevant GSL authorities	Onsite–Contractor District –Local Authorities State – GSL Authorities Overall – PIU (security specialist) (with GSL support)
Safety	As listed in Tables	Contractor–Medial Incident Response Contractor–Escalation to PMU/ CIMT PIU – Inform World Bank	Onsite – Contractor Overall – PIU(security specialist) (with GSL support)
Criminal	As listed in Tables	Contractor – Monitor as per Regional Incident Levels Contractor–Violent Incident Response Contractor–Medical Incident Response Contractor–Hostage Incident Response Contractor Level–Escalation to PIU/ CIMT PIU–Critical Incident Management	Onsite–Contractor/ Private Security Provider Onsite–Local security forces District –Local Authorities State GSL Authorities Overall–PIU (security specialist) (with GSL support)
Extremist	As listed in Tables	Contractor – Monitor as per Regional Incident Levels Contractor – Violent Incident Response Contractor – Medical Incident Response Contractor – Hostage Incident Response Contractor Level – Escalation to PIU/ CIMT PIU – Critical Incident Management	Onsite–Contractor/ Private Security Provider Onsite–Local security forces District–Local Authorities State GSL Authorities Overall–PIU (security specialist) (with GSL support)
Communal Violence	As listed in Tables	Contractor – Monitor as per Regional Incident Levels Contractor–Violent Incident Response Contractor–Medical Incident Response Contractor–Hostage Incident Response Contractor Level –Escalation to PIU/ CIMT PIU – Critical Incident Management	Onsite–Contractor / Private Security Provider Onsite–Local security forces District–Local Authorities State GSL Authorities Overall–PIU (security specialist) (with GSL support)
Vested Interests	As listed in Tables	Contractor –Monitor as per Regional Incident Levels Contractor–Violent Incident Response Contractor–Medical Incident Response	Onsite–Contractor/ Private Security Provider Onsite–Local security forces

		Contractor–Hostage Incident Response Contractor Level –Escalation to PIU/ CIMT PIU – Critical Incident Management	District–Local Authorities State GSL Authorities Overall–PIU (with GSL support)

7.2 ANNEX B: SECURITY REQUIREMENTS IN PROCUREMENT

7.2.1 Overview

Contractor's bidding, and selected, for the delivery of project activities are expected to comply with a number of requirements to ensure the safety of project workers, project affected communities and project assets.

7.2.2 Duty of Care

The PIU on behalf of MoEM and the National Labour laws has an overall Duty of Care to project workers and project affected communities. Contractors selected to deliver activities under the project have a Duty of Care cascaded down from the PIU's overarching duty.

7.2.3 Security Risk Assessment

Prior to beginning work, a contractor should undertake their own security risk assessment to ensure that they are aware of potential causes of risk within an area. This SRA should be retained on file and updated on a regular basis.

The SRA should follow the risk assessment methodology outlined in the project SRA (based on ISO31000) and consider the potential for risks to project personnel, project affected communities and project assets from internal and external sources of risk with the 7 categories identified in the Project SRA (Political, Cultural, Safety, Criminal Activity, Extremist Activity, Communal Violence and Vested Interests).

7.2.4 Security Management Plan

The responsibility for the safety of project workers and project-affected communities should be managed through the implementation of the measures contained in the Project and District SMPs. Where measures cannot be implemented due to prevailing conditions, costs etc. the contractor may suggest alternatives provided these will achieve the same result.

7.2.5 Security Requirements in Bidding Documents

During the submission of bidding documents, a contractor should be able to;

- Demonstrate their capacity to meet and implement all security-related requirements outlined in the Project SRAMP
- Put forward the name of a nominated Contractor Security Focal Point (SFP), along with evidence (CV) of their experience and ability to perform this role;
- Ensure their proposed budget includes a breakdown of costs needed to implement the security measures contained in the SRAMP.

Following successful aware a contractor will be expected to complete an Activity/Site SRAMP based on the measures outlined in the Project SRAMP. This SRAMP will be submitted to the PIU for formal review and approval. The contractor may be required to review and modify (at their own cost) the SRAMP where the PIU finds shortcomings.

7.2.6 Suspension of Delivery Activities

During delivery contractors, in line with the measures outlined in the SRAMP and the Project/District SRAMPs, retain the right to suspend activities where insecurity and risk exceeds their acceptable threshold. The decision by a contractor to suspend activities should be taken after discussions with the PIU, and World Bank, unless to do so would place the lives of project personnel or project affected communities at risk. As part of their Activity/Site SRAMP a contractor will be expected to outline specific triggers which may

lead to the modification or suspension of delivery activities. These triggers may follow those outlined in Tables 44 to 47 of the SRAMP or may take a different form provided they achieve the same end result.

7.3 Annex C: Sample Code of Conduct for Security Providers

This Code of Conduct outlines the standards and principles that security providers, hereafter referred to as "the Company" must adhere to while engaged in providing security services to contractors delivering projects under the project. It encompasses all employees, contractors, and any individual acting on behalf of the Company.

7.3.1 Responsibility and Compliance

Scope - This Code applies to all personnel and third parties associated with the Company.
Compliance Obligation - All representatives must comply with national and international laws, World Bank regulations, and this Code.

Guidance and Reporting - Questions or concerns about the Code should be directed to the Compliance Manager or CEO. Reporting of unethical behavior or misconduct is mandatory, with strict confidentiality maintained.

7.3.2 Ethical, Legal, and Moral Conduct

Legal Compliance - Adhere to all relevant laws, avoiding discrimination, harassment, and unethical business practices.
Moral Obligation - Respect social norms, cultural values, and the dignity of all individuals. Act as ambassadors of the Company, upholding its reputation.
Ethical Business - Conduct business transparently and honestly, preventing any form of conflict of interest or misrepresentation.

7.3.3 Use of Force

Principles - The use of force is a last resort, to be lawful, minimal, and proportionate to the threat.

Reporting - Incidents involving the use of force must be fully documented and reported according to Company procedures and project policies.

7.3.4 Management Commitment and Employee Responsibility

Management Role - Management is dedicated to enforcing this Code, ensuring all business operations adhere to the highest ethical standards.
Employee Accountability - All personnel are accountable for their actions and must familiarize themselves with and follow this Code.

7.3.5 Reporting and Enforcement

Whistle-blower Protection - The Company guarantees protection for individuals reporting misconduct in good faith.
Disciplinary Actions - Violations of this Code may result in disciplinary action, including termination, and possible legal consequences.

7.3.6 Guidance on Ethical Decisions and Transparency

Decision-Making Guide - When faced with ethical dilemmas, personnel should consult with the Compliance Manager or CEO to ensure decisions align with Company values and legal obligations.

Transparency Commitment - The Company commits to operating transparently while maintaining confidentiality and security of information.

7.3.7 Specific Policies

- Human Rights and Labor-Support and respect the protection of internationally proclaimed human rights; reject discrimination, forced labor, child labor, and harassment.
- Health and Safety - Commit to providing a safe and healthy work environment, adhering to all safety regulations.
- Environmental Stewardship - Operate in an environmentally responsible manner within operational constraints.

7.3.8 Personnel Selection, Vetting, and Training

Criteria and Process - Ensure thorough vetting and selection, including background checks and interviews, to uphold the Company's standards.
Training - Provide comprehensive training on this Code, operational procedures, and ethical conduct, especially for personnel authorized to carry firearms.

7.3.9 Conclusion

Adherence to this Code is mandatory for all Company personnel. This document is not exhaustive; personnel are encouraged to seek guidance when in doubt to ensure the highest standards of ethical conduct are maintained.

7.4 Annex D: Rules for the Use of Force/Graduated Force Response

7.4.1 Introduction

These sample Rules for the Use of Force are to be used where a Private Security Provider selected to provide security services in support of the project does not have existing Rules for the Use of Force that meet project requirements.

The Rules for the Use of Force set out guidelines for a graduated response by armed security personnel to any actual, perceived or threatened act of violence against project personnel, locations, assets or communities in which the project operates (and as authorised by the PIU).

No armed personnel shall be deployed in support of the project without a detailed Security Risk Assessment being completed that demonstrates a clear need and that the deployment of armed guards shall not be an alternative to the implementation of structural, procedural or other actions to minimise risk.

7.4.2 Scope

The general requirements of any Rules for the Use of Force should be that they are;

- In accordance with Federal and State law and regulation;
- Consistent with the aim of protecting and defending personnel, communities and project assets;
- Consistent with the use of force only being used when essential and then using the minimum level necessary;
- Allow a graduated response plan which is reasonable and proportionate;
- Clearly define roles and responsibilities of the PIU, Contractor and the security personnel;

7.4.3 Security Provider Obligations

The Rules for the Use of Force should reflect the obligations imposed and agreed under any contract/agreement and should ensure that armed security personnel confirm that they understand these obligations. The RUF should contain guidance that armed security personnel;

- Are trained and qualified to relevant documented standards in the appropriate use of force in accordance with Federal and State law;
- If they use force, it is in a manner consistent with applicable law;
- If they use force, it does not exceed what is strictly necessary;
- Use of force is proportionate and appropriate to the situation;
- Have clear and unambiguous instructions and training on when and how force may be used; and
- Take all reasonable steps to avoid the use of lethal force.

7.4.4 Self-Defense and Inherent Right to Exercise It

The Rules for the Use of Force should reflect that Security Personnel shall always have the sole responsibility for any decision taken by him for the use of lethal force, including targeting and weapon discharge, always in accordance with the Rules for the Use of Force and applicable national law.

Individuals have a right to use reasonable force to prevent a serious crime and the right to use force in their own personal self-defence, and the Rules for the Use of Force reflect these rights as appropriate.

7.4.5 Graduated and Proportional Defense

The Rules for the Use of Force reflect the following guidance on graduated and proportional use of force.

7.4.6 Principles

- To enable the graduated approach and command and control of the situation the force used must be necessary and proportional;
- Respect for human dignity and the human rights of all persons should prevail; and
- Attempts at non-violent means should be applied first.

7.4.7 Non-violent measures

Examples of non-violent means for consideration are:

- Presence – being visible to potential attackers;
- Visual – providing visible warning to deter attackers;
- Sound – the use of megaphones or shouted warnings;
- Show Intent – showing weapons and raising them to indicate intent to use.

7.4.8 Weapon states

Firearms are to be stored securely when not in use and issued only to security personnel on duty. The Rules for the Use of Force consider "states of readiness" for the security personnel. It is suggested that there should be three states for consideration:

- **Normal** – Firearms are issued to on duty personnel with no magazine attached or rounds chambered
- **Heightened** – Firearms have a magazine inserted but no round chambered; and
- **Stand To** – security personnel chamber rounds, but ensure safety catches are applied and are prepared to respond to a threat.

7.4.9 Use of Lethal Force and Opening Fire at a Person

Lethal force should be used only as a last resort and in accordance with the principles referred to above. The circumstances where lethal force in self-defence can be used will vary. Such circumstances may include an armed attack on project personnel, communities, assets or sites where the attackers are, for example:

- Firing directly at persons or persons at a site where the attackers have failed to heed warnings or other deterrent measures (assuming there was sufficient time for such measures).
- Preparing to fire or firing at project personnel, communities, assets or sites whilst clearly demonstrating an intention to draw closer to the site.

If security personnel open fire they should;

- Fire aimed shots to stop the attack;
- Fire the minimum number of rounds necessary to stop the attack; and
- All precautions should be taken not to injure anyone other than the targeted person.

7.4.10Incident reporting and Investigation

States have the primary responsibility to investigate, prosecute or extradite for prosecution persons suspected of committing crimes under national and international law.

In order to implement their obligation to protect human rights, it is necessary to investigate and prosecute potential violations of national laws that aim to protect the right to life. Additionally, the State should ensure that PSPs establish, implement and maintain procedures for the reporting and investigation of any incident, as without such reporting accountability is not possible. In the case of incidents involving the use of force or the use of weapons, any casualties, physical injuries or allegations of abuse have to be promptly reported to the authorities.

The PSP should monitor, and investigate, take disciplinary sanctions and provide remedies where required. Investigations must be conducted expeditiously and impartially, with due consideration to confidentiality and restrictions imposed by national law. The investigation must aim to establish what happened, identify the root causes and determine the corrective and preventative actions that may be taken, including disciplinary sanctions and vetting as required. All incidents investigated shall be reported to the competent authorities. Companies should:

- Report any crimes or reasonable suspicion of crimes, including international crimes, to competent authorities;
- Prepare incident reports whenever PSP personnel are involved in using a weapon;
- Establish incident monitoring, reporting, investigation, disciplinary arrangements and remediation procedures, particularly for cases involving the use of force and/or weapons.

7.4.11Project Level Incident Reporting Tool –Template

Incident reporting- as per the Security Management Framework and WB ESIRT, all ES incidents that have or result impact to the project personnel, workers, activities, communities, contractors and WB/MoEM reputation will be reported within 24 hours of their occurrence, typical or same WB ESIRT will be applied by the project. This tool will be confidential, owned and managed by the SA/SF while its utilization orientation/training will be conducted through the Bank's technical person/unit. WB will include the recipients of those incidents reported

7.4.12Estimated Budget

The estimated budget for the implementation of the SRAMP presented below. Specific activities will be submitted to EAPP-PIU and MoEM in time for approval before the activities are conducted. Detailed costs will be included when the contractors prepare their site-specific SRAMPs. The requirement to be prepare the site-specific plans will also be reflected in the contract/bidding documents.

Table 7-2. Budget Estimate

Item	Responsibility	Cost (USD)
Training/awareness of law enforcement personnel and workers/employees.	PIU/Contractor	191,000.00 **N/B** The cost will be prepared when contractors prepare site specific SRAMPs.
Provision of physical security	Contractor	Estimated costs: 500,000 **N/B**

		The cost will be prepared when contractors prepare their site specific SRAMPs.
Surveillance and access control	Contractor	Estimated costs: 300,000 The cost will be prepared when contractors prepare their site specific SRAMPs.
Recruitment of and training of security guards	Contractor is responsible for payment of the monthly salary of security guards/security agencies and per diems for local security officials for their technical assistance as well as additional training and orientation of recruited guards.	Estimated costs: 200,000 The cost will be prepared when contractors prepare their site specific SRAMPs.
Law enforcement support	Local police assigned to patrol the sub project sites whenever necessary. Contractor can request for additional forces to be assigned conditionally.	The budget for the local police force will be handled by the police service. (No separate budget is required). However, if the local police are assigned upon the request of the Contractor, he/she shall be renumerated by contractor
Large-scale events such as criminal activity, demonstrations, civil disorder and which is not specifically associated with the project.	Security Apparatus (Defense Forces and PS) in collaboration with the security guards of the Contractor.	Somaliland government is responsible for covering any costs related to securing the subproject areas.
Monitoring SRAMP Implementation	PIU	30,000.00

7.5 Annex E: SECURITY OPERATING PROCEDURES

Common Operating Procedures

Physical Security

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

Communications

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

Construction Security

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

Fencing

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

Exterior Lights

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

Security Guards

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

Project Vehicles

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

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

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

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

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

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

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

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

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

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

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

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

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

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