United Nations
Department of Peace Operations
Ref. 2021.03

Guidelines

Force Protection for Military Components of United Nations Peacekeeping Missions

Approved by:	Jean-Pierre Lacroix, USG DPO
Effective date:	*September 2021*
Contact:	*Office of Military Affairs*
Review date:	*September 2024*

DPO GUIDELINES
ON
FORCE PROTECTION FOR MILITARY COMPONENTS OF UNITED NATIONS PEACEKEEPING MISSIONS

Contents:

ANNEXURES

A. PURPOSE AND RATIONALE

1. These Guidelines provide Member States, Troop Contributing Countries (TCCs) and uniformed personnel with practical guidelines on Force Protection (FP). The document provides a generic set of planning, training, coordination and implementation considerations for FP. Implementation of these guidelines is intended to aid in coherent, comprehensive and effective FP which will improve safety and security of troops.

2. UN peacekeeping operations face increasing challenges that undermine the ability of UN missions to fully deliver on respective mandates. With the growth in complexity of operations, there is an increase in the multi-dimensional nature of UN peacekeeping operations resulting in a dynamic, evolving set of threats. Asymmetric complex attacks targeting peacekeepers, UN facilities and UN operating bases remain persistently high resulting in fatalities and injuries of peacekeepers. Direct targeting of peacekeepers has undermined the tacit protection previously afforded by the wearing of the symbolic blue helmet or the painting of equipment in white with UN logos. Safety and security of peacekeepers remain a strategic priority in the action for peacekeeping initiative with ongoing efforts driven by the Santos Cruz action plan to decrease fatalities due to malicious acts. FP measures and considerations in peacekeeping missions must reflect the changing environment and be continuously reviewed and updated.

3. Primary responsibility for the security and protection of personnel deployed through the UN system and organizational property rests with the Host Government. The UN has a responsibility to reinforce and, where necessary, supplement the capacity of the Host Government to fulfil these obligations. The UN has a comprehensive system on safety and security which includes the UN Security Management System (UNSMS). UN civilian personnel and individually deployed military and police personnel are covered by the UNSMS. Security of troops with their contingents is covered by separate FP mechanisms that encompass the capability of military units to manage risks and protect themselves from prevailing threats and hazards.

4. Military contingents are responsible for delivering diverse mandated tasks which may include protection of UN personnel, personnel of non-UN agencies in support of field missions, as well as Protection of Civilians (PoC). Often these activities are carried out in a challenging security environment. Hostile actors will strive to exploit the perceived or actual vulnerabilities of UN troops, UN bases and facilities, and will initiate actions to disrupt the mandate implementation. This necessitates that military contingents identify the threats, understand appropriate FP measures and procedures to manage these risks and emplace mitigation measures to minimize loss of UN personnel and property.

B. SCOPE

5. These guidelines on FP include fundamental principles and operational guidance on measures to minimize the vulnerability of UN troops, facilities, equipment, materiel, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness.

6. In these guidelines, FP is not limited to physical protection of troops, facilities or protection during movement, but also includes actions for mitigating other hazards and threats, such as information security, medical exigencies, fire, and explosive ordinance (including mines, improvised explosive devices (IED) and explosive remnants of war).

7. These guidelines apply to all formed military units deployed in UN peacekeeping operations, staff of Force/Sector HQs, personnel of the Department of Peace Operations (DPO) in the field and at United Nations Headquarters (UNHQ) as well as key personnel of TCCs, decision makers and planners who shall use these guidelines as reference as they plan, train and prepare contingents for a UN peacekeeping operation. The Guidelines may also serve as a reference for personnel of the Department of Political and Peacebuilding Affairs (DPPA) and special political missions. In addition to these guidelines, deployed FP units may be required to add additional requirements to their mission set based on the environment and tasks.

8. These Guidelines reference mandatory requirements as required by operating in a UN field mission as well as recommended or discretionary approaches, which are denoted throughout the guideline via ‘shall/shall not’, ‘should/should not’ and ‘may/may not’, respectively.

C. GUIDELINES

C.1 Definition of Force Protection

9. FP is the cyclic process of detecting threats and hazards to UN personnel, facilities, resources, operations, activities, and assessing their risk in order to apply pro-active and reactive risk mitigation measures. These measures include threat prevention, pre-emption, negation, mitigation and response to preserve the freedom of action and operational effectiveness thereby contributing to mandate implementation and mission success.

10. **FP is a fundamental principle of all military operations** and a way to ensure the survivability of the UN military contingents. It includes measures and means to identify, prevent harmful events and/ or minimize the vulnerability of UN troops, facilities, resources, operations, and activities from threats and hazardous events. FP measures can either be used to prevent vulnerabilities from being exploited or mitigate the impact of a vulnerability that has been exploited, or both.

11. FP includes a systematic risk management process that identifies risk to personnel, equipment and mission, followed by the timely development and implementation of measures to manage the risks to UN military personnel, units, bases, facilities, equipment, materiel, as well as during military operations, tasks and activities.

C.2 Principles of Force Protection

12. Analysis of the operating environment[1], mission analysis[2] and commander's intent provide the starting point for the identification of FP requirements and procedures. FP implementation then aims to preserve the potential of UN troops by countering the wider threat for all contingent elements (i.e. personnel, equipment, environment) from exploitation by an adversary, or natural and manmade hazards. As such, FP should be guided by the following principles:

12.1 **Interoperability.** Effective FP integrates all force components and includes necessary coordination and cooperation with all other mission components (civilian and police), UN partners, Host Government, when and as necessary, within and outside the area of operations (AO), and addresses all aspects of the threat or hazard. Interoperability should be achieved through continuous liaison, cross training, the establishment of coordinating measures, and rehearsal of these measures both within the force and mission wide. Interoperability is to be achieved through the conduct of operations, equipment, communication, training, as well as Tactics, Techniques and Procedures (TTP). This type of comprehensive approach will allow the implementation of effective, collaborative, multi-service protection measures across a wide spectrum of scenarios identified through the risk management process.

12.2. **Prioritization**. FP must balance the need to preserve force capability while implementing the mandate. It is unlikely that the capability will exist to protect all force elements and resources to the same degree. Priority should be given to the protection of Force/mission success, both tangible, such as lines of communications (LOCs), and intangible, such as operational cohesion or political will.

[1] United Nations Military Peacekeeping-Intelligence Handbook, April 2019, Chapter 9.
[2] United Nations Infantry Battalion Manual, January 2020, Chapter 2

12.3. **Flexibility.** FP measures should be developed with the capability to be flexible and respond to a rapidly changing threat while accounting for resource limitations. FP requires flexibility to allow operational forces to develop standards and procedures to ensure individual and collective needs are still met.

12.4 **Unity of Command and Control**. An effective command, control and coordination structure that is inclusive of all force elements is essential for FP. Failure to ensure FP as a result of weak command-and-control structures, incorrect mindset, negligence or insufficient levels of compliance can compromise overall mission success and mandate implementation.

12.5. **Response.** Swift action and/or the quick movement of forces may be required to prevent harm to UN troops or damage to UN equipment. The level of response may be elevated to lethal force depending on the level of threat, principles related to the use of force and respective Rules of Engagement (ROE).

12.6. **Sustainability.** Sustainability includes the ability to maintain a standard level of FP posture over a long period of time. FP efforts shall be sustained at all operational levels and during military operations, engagements, and activities. Sustainability of FP measures ensures that freedom of action of troops in all operational and supporting activities is maintained.

12.7. **Proactive Posture**. A proactive posture should be intelligence-led and dependent on comprehensive risk assessments and the willingness to take the initiative to deter, prevent and respond to threat events. Troops shall maintain the right mindset to ensure a high level of situational alertness and a high operational tempo, physically dominating key or decisive terrain by patrolling, conducting temporary operations and using complementary equipment. A proactive approach to FP is essential and will often involve joint actions implemented through the coordination and synchronization of operations, intelligence, information and outreach activities. Outreach activities should include an assessment of the strength and weaknesses regarding relationship with the local population.

C.3 Nature of Force Protection

13. FP is a basic responsibility during missions and applies to all units especially those that conduct security tasks. Specific protection tasks for UN personnel and facilities shall be defined for each mission in accordance with crisis management arrangements. For further information see the United Nations Infantry Battalion Manual (UNIBAM).

14. FP related activities shall be exercised in full compliance with UN standards of conduct, including ST/SGB/1999/15 on Observance by UN Forces of International Humanitarian Law, mission specific ROE and the mission status-of-force agreement.

15. FP is essential to all operations, and therefore senior mission leadership shall ensure that all military units can defend and protect themselves appropriately against prevailing threats throughout the operational environment.

16. FP shall be cross-organizational and multi-dimensional, providing multi-layered protection of forces and resources. To ensure multi-layered protection, a broad array of integrated functional expertise is necessary, which shall include, but is not limited to: Peacekeeping-Intelligence

collection, analysis and dissemination, deterrence and preventive posture, effective command and control, communication, physical security enhancements, armed defense, law enforcement liaison and a swift but graduated response. In this FP posture, troops shall always be on alert and ready to counter any sudden escalation of threat no matter the existing security state. A breakdown of the basic components to be employed include:

16.1 **Situational Awareness**. Knowledge, understanding and anticipation of a situation through monitoring and reporting of current events, analysis and forward-looking assessments[3] is essential to FP. Situational awareness is an important responsibility of contingents in their area of responsibility (AOR). In coordination with the Joint Operation Centre (JOC), Joint Mission Analysis Centre (JMAC) and Security Information and Operation Centre (SIOC), a comprehensive AOR situational awareness and understanding is required to support the ability of senior mission leadership to identify, prevent, mitigate and/or respond to threats to UN Forces.[4] [5] Situational awareness platforms such as Unite Aware and situational awareness database such as UN Sage Incidents/Events Database System shall be used to record, share, and monitor information on incidents events and movements.

16.2. **Peacekeeping-Intelligence**. Analysis of information, trends and technical intelligence to determine the threats (past, present and future) should be reviewed and analyzed on how best to mitigate these threats. The ability to monitor, gather and share information, analyze, maintain heightened situational awareness and report, with a focus on early warning and response mechanisms, is critical. Continuous access to timely, relevant, accurate, all-source Peacekeeping-Intelligence is central.[6]

16.3 **Prevention/Deterrence**. Prevention/deterrence includes activities undertaken when no specific direct threat has been identified (latent threat). Military contingents should contribute to a general deterrence posture by conducting routine tasks, such as check points, patrols, terrain dominance, information gathering and analysis. They should also strengthen community-oriented approaches and promote engagement with communities in compliance with the "Do No Harm" principle. Since the primary responsibility for the security and protection of personnel employed through the UN system and the organizational property rests with the Host Government, prevention activities can include support to the strengthening of host-state capacities, within the ambit of Human Rights Due Diligence Policy (HRDDP), to respond to threats posed by local non-state armed personnel/ groups to UN troops and property.

16.4 **Effective and Accountable Mechanisms of Command and Control**: It is the responsibility of commanders of all contingents and units to ensure that FP measures are implemented by all subordinates. Commanders shall ensure those under their command understand and comply with the ROE. The Force Commander (FC) is ultimately responsible for enforcement of force protection measures. An effective command-and-control structure would ensure the efficacy of FP.

16.5. **Communication**. Communication includes the reporting of information and checking to ensure the message (whatever format) was received and understood.

[3] Policy on United Nations Joint Mission Analysis Center, 2020, page 14
[4] United Nations Infantry Battalion Manual, January 2020.
[5] United Nations Military Peacekeeping Intelligence Handbook, April 2019, Chapter 1.
[6] Ibid. (see footnote 4 and 5).

Communication channels should be secure to maintain information security and ensure access to critical information is restricted.

16.6. **Physical Security**. Physical security consists of physical measures designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm. FP physical security requirements may vary from mission to mission and may also evolve over time. Adjustments to physical security requirements will be required based on periodic security assessments. Details on physical security is at Annex A to this guideline and the Contingent Owned Equipment (COE) Manual.[7]

16.7. **Equipment**. FP equipment, coupled with FP measures should allow UN forces to counter equipment, capabilities, TTPs used against UN personnel and facilities. FP equipment might include but is not be limited to portable or vehicle-mounted electronic counter-measure jammers, motion detectors, day and night vision surveillance equipment, tactical unmanned aerial systems (UAS), indirect fire detection sensors, electronic trackers, mine resistant ambush protected vehicles, mine path clearing system, warning systems and various types of movement sensors. The deployment of COE required for FP purposes will be determined on a case-by-case basis informed by the relevant statement of unit requirements (SUR) and mission-specific requirements.[8]

16.8. **Law Enforcement Liaison**. Military contingents shall establish a link or conduit with UN police, Department of Safety & Security (DSS), host nation security forces and other law enforcement agencies.

16.9 **Civil-Military-Cooperation.** Commanders and units should establish reliable, open-minded, trustful and bi-directional contact and communication to the government, governmental organizations and other important role players through the appropriate channels.

17. The relative contribution of the fundamental elements of FP will be determined by the threat, scale of operation and environment. Details of the fundamental elements of FP are at Annex B.

C.4 Authority, Command and Control

18. The FC reports to the Head of Mission (HOM) and is responsible to him/her in the discharge of his/her functions. The FC exercises “UN operational command and control” over all UN military personnel and units in the mission and establishes the military operational chain of command.[9] The FC places military units and individually deployed experts under the command of subordinate commanders, which allows subordinate commanders to assign tasks to forces under their command.

19. FP is a command responsibility and the overall responsibility for FP in the mission area is with the FC.

---

[7] Manual on Policies and Procedures concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions, page 53and Chapter 3 Annex B and Appendices

[8] Refer to COE Manual, Chapter 3, Annex A (A/75/121)

[9] DPO-DOS Policy on Authority, Command and Control, 2019.

20. Subordinate Commanders are responsible for the establishment of FP plans within their sectors/units that meet the intent of this Guideline. Commanders must abide by the alert status as determined by the Force HQ. Subordinate commanders may further impose stricter Alert States (see Annex E) and associated protection measures based on their assessments but may not go below the higher-level command's FP posture without FC's authorization.

21. A working group on FP issues at FHQ is to be led by the Force Chief of Staff (FCOS).

22. A FP officer/focal point should oversee, coordinate, and monitor FP issues (primary focal point for policy and coordination within their HQs) and report any issues or policy changes to the Force Chief of Staff.

D. FORCE PROTECTION PROCESS

23. The FP plan is not intended to replace the Operation Plan (OPLAN) but rather to provide FP planners and commanders with a logical process to successfully manage FP at its lowest practical level.

24. The FP process is to provide military decision makers and FP planners with a methodology to assess threats, hazards, and plan implementable FP measures at all levels. The process consists of mission analysis, threat and hazard identification, risk assessment, development of FP measures, tasks and activities, as well as execution (implementation).

D.1 Mission Analysis.

25. The UNIBAM provides details on mission analysis. In analysis of the mission, FP planners would focus on FP matters. Any tasks and actions identified through mission analysis that fall within the FP basic components should be covered in detail in a FP annex to the OPLAN.

D.2 Threat and Hazard Identification.

26. This is the identification of those actors, factors and actions in the operations area that may potentially cause harm. identification consists of providing an objective description of the prevailing security threats and hazards in the area. The FHQ is responsible for identifying threats for the mission area at the operational level. In addition, units must identify threats within their respective AOR.

D.2.1 Threat and Hazard Assessment.

27. A threat/hazard assessment is the intelligence assessment of threats and hazards in the area of operation. It requires the fusion of information and Peacekeeping-Intelligence from military, police and civilian sources. Threat assessments determine the targets, perpetrators, capabilities, most likely and most dangerous courses of action, and overall intentions of identified threats. While an overall integrated threat assessment is required at the FHQ, Sector commanders should also analyze and disseminate threat information to subordinate commanders focused on their respective deployment area. Additional threat assessments should be conducted at Sector and Unit levels. Threat assessments at Unit level should be communicated to Sector and FHQ.

28. For each threat/hazard, the following elements should be determined:

- Situation and type of threat (What);
- Potential perpetrators/hostile actors (Who);
- Potentially affected groups (Against whom);
- Areas targeted by possible attack (Where);
- Days and time attacks are most likely (When);
- Motivation (Why);
- Possible movements and tactics of hostile actors (How).
- Potential effects from weather or environmental conditions/changes

29. Planners should assess the intent, capabilities, and the danger level of potential perpetrators for each identified threat event.

29.1. Intent: Planners should access the intention or disposition of a threat event to cause harm.

29.2. Capability Assessment of Potential Perpetrators or Hostile Actors: Planers should assess threat capabilities to determine the ability of potential threats to cause harm. The assessment should consider threat structure, leadership, professionalism, tactics, weaponry, targeting and logistics.

29.3. Danger level of Potential Perpetrators or Hostile Actors. Each of the potential perpetrators should be assessed for their threat level by looking at their capabilities, intentions and historical background.

30. A threat assessment should be based on accurate and timely peacekeeping-intelligence which serves as the basis for the selection of the proper security alert state and associated FP measures.

31. The threat assessment also provides the FC with situational awareness that reduces the probability of surprise, enhances decision making, and enables effective management of the operational environment thus enhancing the overall effectiveness of the force. Annex C provides a guide for defining the threat environment level (i.e. low, moderate, etc.) in accordance with the UN Security Risk Management Process.

D. 2.2 Vulnerability Assessment

32. A vulnerability assessment enables planners to determine the susceptibility of personnel, facilities or assets to attack or degradation due to hazards. Planners shall assess vulnerabilities to identify deficiencies and/or weaknesses that render their personnel, bases, facilities, materiel or mission vulnerable to a range of known or possible threats or hazards.

D.3 Risk Assessment.

33. Commanders at all levels should prioritize threats in order to identify those situations where force protection action or risk mitigation is most needed. This process of prioritizing threats is facilitated by a risk assessment, which determines (a) the likelihood a threat materializes, and

(b) the impact the threat would have if it materializes. The combination of these two factors allows commanders and staff to determine the risk associated with each threat identified.

34. The willingness to accept risk is scenario dependent. The risk tolerance/threshold of the force is defined by the FC and or unit commanders according to the capacity of the Force, Unit, Mission's plans or other agreements. The risks from threats and hazards should be continuously re-evaluated to ensure appropriate FP measures are always in place. Although it is not possible to protect every asset against every threat all the time, those assets identified as "critical to the mission" shall be protected as a first priority.

35. Risk assessments as well as visual tools such as tables and maps, need to be updated routinely or whenever the situation in the area of operations changes. The FHQ/SHQ should maintain a Risk Analysis Matrix table, units should consult with the higher headquarters when compiling their risk assessment. See Annex D for more details.

D.4 Develop Force Protection Measures, Tasks and Activities

36. Following a risk assessment, FP measures, tasks and activities should be identified, developed and analyzed. After FP measures are put into place, hazards are re-assessed to determine any residual risk. FP measures, tasks and activities are to prevent, pre-empt and negate, identified threats with the aim to reduce or eliminate the risks posed on the force. FP measures should reduce the likelihood and impact of the threats and hazards identified.

D.5 Execution/Implementation

37. Once the FP measures, tasks and activities are developed they are to be implemented. This is achieved by converting FP controls into clear and simple execution orders, establishing proper authorities and accountabilities and providing the necessary support to implement while remaining fully aware of any residual risk. The implementation plan should have clear responsibilities for each component of the force. Some measures and activities related to assigning alert states, dress codes and vehicle movement codes are described in Annex E.

38. FP planning should culminate in a clear implementable plan as an Annex to the OPLAN, and subsequently translated into fragmentary orders (FRAGOS), standard operating procedures (SOPs), directives and instructions for implementation. Mission specific FP SOPs should have specific measures of FP for bases, patrols, convoys, etc.

39. Each level of command is required to implement FP measures, tasks, and activities based on the mission and threat situation. The same measures, tasks, and activities may not necessarily be implemented by all units in the same theatre. Therefore, coordination is necessary across all levels to provide adequate and synchronized FP.

D.6 Monitor and Review.

40. Monitoring and reviewing should occur throughout the FP process to review actions, identify new weaknesses and to make changes or adjustments based on changing situations or events. Periodic reviews are required to validate the effectiveness of the FP plan.

41. Monitoring and reviewing ensures FP measures, tasks and activities are implemented and executed in a standardized manner and that a feedback mechanism is in place. Review

tools/means such as FP evaluations, surveys, and exercises should be used to identify FP deficiencies and shortcomings.

42. Accurate reporting and feedback mechanisms ensure timely resolution of identified weaknesses. Lessons learned/identified, and best practices identified should be shared across the FP stakeholder community through FP after action reviews, end of mission reports, briefings, doctrine development, training, and exercises. Commanders and staffs at all levels should continuously monitor threats, hazards, vulnerabilities and their own FP posture, and immediately take appropriate corrective action when required. The FP process is described in Figure 1 below. Details of the UN Security Risk Management Process is outlined in the Security Risk Management Manual (2019).

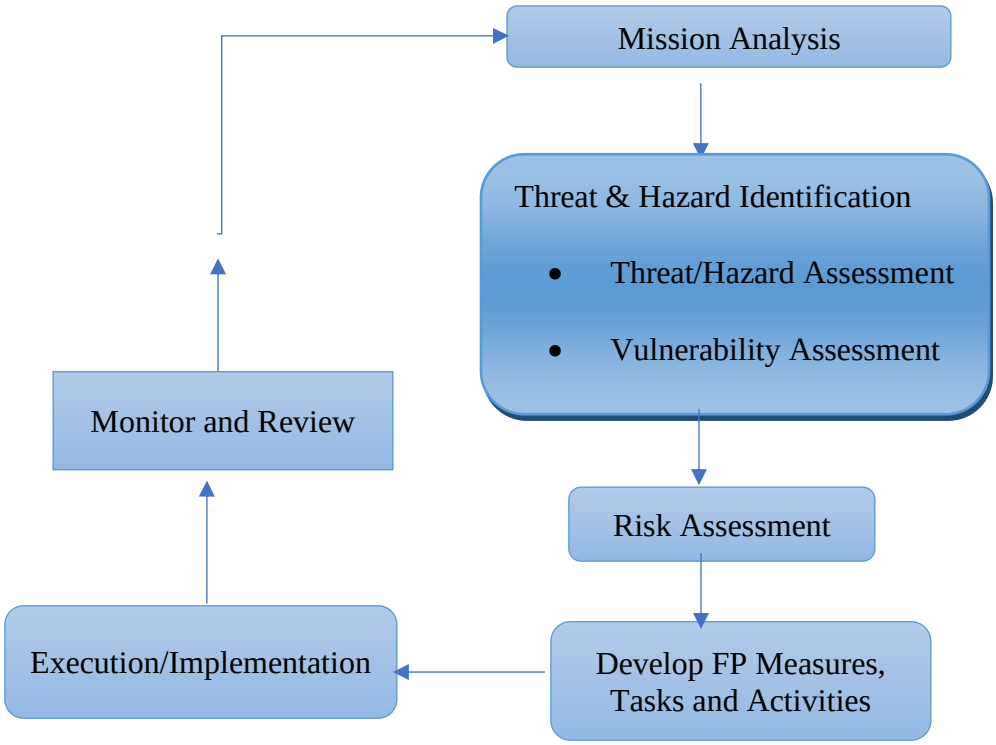


Figure 1: Force Protection Process

E. PROCEDURE

E.1 Force Protection Planning

43. FP planning is the procedure of identifying necessary measures to reduce or mitigate threats, hazards, vulnerabilities and risks in a mission or operational area. FP should be a key consideration in all peacekeeping operations, thus military contingents shall factor in FP at the outset of the planning process in a mission.

44. FP planning should include identifying a full range of threats and hazards across the range of operational activities. Based on the identified threats and hazards, FP measures should be integrated into all plans and contingency plans. During the pre-deployment phase, threats and

hazards should be identified and planned for by the TCC providing its troops with the appropriate FP assets and capabilities required during deployment. The threats should be constantly analyzed and new threats identified to determine if FP measures remain adequate or require adjusting, and during post-deployment, lessons should be identified and incorporated into future national planning processes.

45. FP plans should establish the FP organization, command and control, delineation, appropriate resources and capabilities required, mitigation measures, responsibilities and be incorporated into the conduct of operations. Annex C identifies possible threat environments across six levels from low threat to extreme threat.

46. FP planning considers threat and vulnerability assessments to provide a basis for determining FP measures, mitigation, tasks and activities that should be planned for in protecting personnel, facilities and critical assets in each respective mission or threat environment.

47. All commanders shall contribute to the Mission wide protection planning process. The wider protection plan of the mission includes non-military personnel, contractors, civilians and non-governmental organizations and their facilities which by UN mandate or agreement are entitled to protection by UN forces. The FP planning process should not only focus on physical protection of a base or convoy but should be all-inclusive, and include potential threats such as, but not limited to, medical and environmental exigencies, fire and lightning, explosive ordnance, Chemical, Biological, Radiological and Nuclear (CBRN), cyber and information technology threats. Though each FP plan relates to a particular environment, it should consider mission-wide/strategic level risk mitigation measures to ensure standardized protection against crosscutting threats in the mission. These FP plans should be reviewed periodically or as necessary to assess continuing applicability to the nature/level of threat or vulnerability in order to mitigate the risks and plan effectively. FP plans shall ensure assets identified as critical to the mission are always protected. **Proper FP planning will help commanders achieve the required balance between risk mitigation and mission accomplishment**.

48**. Operating Base Force Protection Plan.** While planning the establishment of an operating base (temporary or permanent), appropriate UN senior leadership shall assess and consider the emplacement of effective physical security measures early in planning process. Base FP plans should be developed and integrated during the planning process that establishes an operating base. The FP plan will vary according to the operating environment but should generally be comprised of a threat scenario encompassing non-compliant armed groups, terrorist actors with asymmetric capabilities, armed conflict, crime and a vulnerable local population. An operating base should be sited to maximize FP and should be capable of deterring, detecting and denying unwanted access to UN facilities or advance. Commanders shall ensure consideration for defensive planning in preparation of bunkers; protection for accommodations, sectors of fire; establishment of entry control points; utilization of sensors etc. as outlined in the UNIBAM.

49. **Assets (Facilities/Equipment/Materiel) Force Protection Plan.** Requirements of FP for facilities, equipment and materiel will vary according to the operating environment, threat and location of assets. Plans should include measures, tasks and activities to protect assets organic to unit and any assets that have been attached to it by higher level. Planning should include considerations for appropriate blast protection and explosive detection capabilities such as explosive detection dogs or chemical detectors.

50. **Convoy and Escort Force Protection Plan.** Threats are usually more pronounced during mobile operations and in some missions, most of the casualties occur via asymmetric and IED

attacks during movements.[10] Assessments and planning of convoy/escort operations requires support, coordination and cross-communication between all security components and FP stakeholders. Planning for convoy/escorts should always identify the potential threats along the route such as ambushes, indirect fire, IEDs, land mines or other explosive devices that may be encountered during the operation.[11] Planners should consider measures to counter the identified threats by identifying primary and alternative routes, random timings, providing a stand-by quick reaction force, share intelligence reports around the areas of movement, use of relevant equipment (refer to COE manual) and vehicle movement codes. **Plans should include route clearance patrol when the threat warrants it.**

51. **Patrol Force Protection Plan.** Proactive patrolling by day and night in order to dominate the environment and ensure Protection of Civilians and mandate implementation is a critical task. FP plans shall include personal security and protection of troops on patrol as well as possible threats from small arms fire, IED, land mines and indirect fire. Patrol plans should include considerations for different times and different routes so that a pattern is not established. In integrated patrols, (military with police and or civilian guard), planning should include considerations for risk tolerance/threshold and the protection of other components in the integrated patrol.

52**.** **Checkpoint Force Protection Plan.** Depending on the situation, checkpoints may include UN Police and/or local police as well as security experts from the civilian components of the mission Requirements for FP at a checkpoint would vary according to the operating environment and threat. FP Plans should at the minimum include considerations for adequate cover, and fields of fire.

E.2 Contingent Force Protection Planning

53. Military contingents should be able to:

- Ensure individual and collective FP to all force elements in the AOR, whether such force elements are mobile or static.
- Maintain its bases in a state of good condition and repair.
- Ensure planning considerations for FP are in line with the mission concept of operations (CONOPS).
- Develop and implement FP measures and activities consistent with identified threats, both direct and indirect. FP personnel (together with engineer unit/personnel) plan responsive and preventative measures, including planning calibrated responses that minimize collateral damage.
- Develop and rehearse contingency plans for operating base (temporary/permanent) protection, including conducting emergency drills or simulated scenarios about reaction to hostile actors, adversary attacks, fire-fighting drills, and natural disasters.

[10] Lieutenant General (rtd) Carlos dos Santos Cruz report on Improving Security of UN Peacekeepers: We have to change the way we do business. December 2017.
[11] Guidelines on Improvised Explosive Device (IED) Threat Mitigation in Mission Settings. Para 23

- Develop and rehearse contingency plans, including table-top exercises or stand-to drills and reaction to adversary attack/ambush.

- Ensure FP plan is provided to FHQ/SHQ and report any adjustments made to the plan. All changes to alert states, dress codes etc. should be reported and it should be ensured that they do not fall below the minimum levels (as set by the FC). See Annex E.

E.3 Force Protection Training

54. Appropriate FP training for military personnel is vital to the survivability of troops and the success of any mission. Training should include Pre-deployment training, Induction and Ongoing trainings such as refresher trainings/activities/drills/workshops.

55. Individual and collective pre-deployment training remains a national responsibility under General Assembly resolution A/49/37 and in accordance with the Policy on Training for all UN peacekeeping personnel. Induction and ongoing training of the military component, supported by a meaningful evaluation and assessment process, is the responsibility of the Force, Sector and Unit Commanders. DPO and DOS play a role in peacekeeping training, by developing relevant doctrinal concepts and standards as well as providing supporting pre-deployment training materials and follow-up in-mission training coordinated by the mission's Integrated Mission Training Centre.

56. The scope, type, methodology, length, frequency, and execution of all FP trainings should be conducted in accordance with UN standards and mission specific guidance. FP trainings should be comprehensive and designed with a threat-based approach. FP training modules should be tailored to the unit's AOR to the best extent possible. It should include intentional and unintentional threats, including direct and indirect attacks to static or mobile positions, IED action, land mines, explosive remnants of war, natural disaster, fire safety[12], CBRN awareness, spread of infectious diseases among others. Maintaining IED and CBRN awareness is important whether the threat is present or not within a specific mission at the time of deployment. Training should include awareness on IED emplacement identification and route clearance operations. For more information see DPO-DPPA-DOS Guidelines on Improvised Explosive Device Threat Mitigation in Mission Settings. Pre-deployment training should ensure that forces are interoperable with UN forces, mission elements and security entities once deployed.

57. Upon deployment, induction training and awareness generation sessions should be conducted to reinforce some of the pre-deployment training and planning efforts and is critical to the integration of FP procedures on a multinational/multidimensional level. All personnel should be briefed, as a minimum, on the location-specific and mission-wide threats and be conversant with the early warning indicators and mechanism as well as the risk mitigation actions in place.

58. In-mission FP training should include joint training and synchronization of procedures with other UN components to support interoperability and an integrated approach. Joint training should be conducted as a minimum, quarterly and done in collaboration with UNDSS. Training should include adaptive tactical and contingency planning and should be threat-based and within the available resources.

[12] United Nations Fire Safety Guidelines-United Nations Security Management System (UNSMS) 28 June 2021.

59. Military units should conduct, as a minimum, monthly FP exercises that include rehearsals for FP scenarios such as defense plans for mobile and static operations, insider threat, direct attack, etc. and all possible preventive and reactive risk mitigation actions and measures.

60. During operations or under high-risk situations, troops may require higher frequency of rehearsals and review of their defense and protection plans.

E.4 Evaluation and Validation of Force Protection

61. UNHQ should ascertain TCC preparedness during possible assessment and advisory visits, and the pre-deployment visits (PDVs) based on standardized criteria[13] in advance of each contingent's induction, in line with the Operational Readiness Assurance and Performance Improvement Policy.[14]

62. The FC should ensure FP is evaluated during deployment of units/contingents. Evaluations should include physical security measures, equipment, information security, and the proactive security measures practiced by units. Force and sector commanders should review and, if validated, approve the defence plans of their subordinate units. In some cases, the FHQ and SHQ should inspect the readiness of their units to be protected, while static and mobile.

63. Validation of FP is to be conducted during rotation of contingents through self-certification by the TCC and in special occasions (if mandated by the USG or Military Adviser) through a UNHQ team. Validations should examine the After-Action Reports and Lessons identified from recent security related events in the Mission and validate the mitigating measures implemented by the Unit. Validation should examine the effectiveness, adequacy and scope of the overall FP plan, ensure that risk controls are implemented to standards and ensure that a feedback mechanism is in place.

64. In each mission, a Force Protection Assessment (FPA) is to be conducted quarterly in collaboration with UNDSS and a corresponding FRAGO released with orders and records of any remedial action required. The FPA should be conducted regularly with a focus on identified threats and the mitigations measures as well as potential new threats. After every FPA, the FP SOP should be reviewed as necessary. The FPA should address the following areas:

64.1. **Plans and Training**. Plans should include ways of implementing FP, procedures and plans for the conduct of regular FP exercises. A FP plan as described above in Section E.1 of this Guideline should be prepared. A review of overall security awareness and assessment of the ability to train individuals and teams prior to travel, convoy movements or deployments elsewhere in/out of the AOR should be included in the plan.

64.2. **Command, Control, Communications, Computers and Intelligence (C4I)**. Review unit and/or mission C4I arrangements to confirm that adequate facilities and procedures are in place. Reviews should include operational status of both technology and equipment and operators' capabilities; basic communication means should be functional, networks should be up to proper security requirements, and personnel who require access to information systems (such as Unite Aware) are properly vetted, trained and know how use the system. Daily radio checks should be conducted in order to verify communications between units, sectors and

[13] Standardized criteria can be directly requested from the Office of Military Affairs/ Military Performance Evaluation Team (MPET) who maintain a database.
[14] ORA Policy ref.2015.16/UN DPKO/DFS/01 Jan 2016.

respective HQs in mission area. Stand-by satellite phones are to be part of the communications equipment inventory for every unit as an emergency communication system. Information security should be safeguarded by complementary procedural, personnel, physical, and information security measures. Measures may include, but are not limited to communications security, emission security, and computer systems security.

64.3. **Early Warning and Intelligence**. Threat intelligence support should include the ability to receive and disseminate threat information, and how threat information supports implementation of appropriate FP measures.

64.4. **Inter-unit Coordination and Cooperation**. Integration of local community, host nation, neighboring units and tenant organization information into FP plans. Evaluate the level of support and integration of all elements in and around an activity or installation in order to enhance FP measures in a mutually supporting manner and to respond to any situation or threat/hazard. Additionally, review the status of agreements in effect to formalize these arrangements.

64.5**.** **Perimeter Integrity**. Consider physical security techniques and facilities to include perimeter security, intrusion detection devices, entry access control, fences, lighting, barriers, alarm systems, and other means that can increase the level of security.

64.6**.** **Infrastructure.** Review infrastructure and assessment against known threats to ensure that adequate infrastructure is available and afforded appropriate security measures.

64.7**.** **Information Security and Operational Security**. Ensure that procedures are in place to protect information and that SOPs are enforced. Periodic training should be emphasized to ensure understanding.

64.8**.** **Mobility**. Review procedures for the preparation, planning, conduct of, and equipment requirements for movement within the AOR.

64.9**.** **Fire Plan**. Review fire plan (direct, indirect, illumination) and associated assessment against the pending threat. Review should include evacuation plans.

64.10**.** **Aircraft Operations** Review procedure for protection of helipads and support to aircraft movement. Review to include physical security measures, equipment support, adequate lighting and number of personnel.

64.11. **Medical Provision**. Ensure there is adequate provision to respond to health threats and hazards. Provisions should include preventive measures against diseases.

64.12 **Reinforcement** Review arrangements for reinforcement or quick reaction units**.**

64.13 **Recuperation**. Review arrangements for recuperation. Provisions to include minimum effective timing and reconstitution of units and equipment before subsequent operational deployment.

E.5 Force Protection Organization/Coordination

65. FP require forces to have robust and flexible command and control capabilities. It demands, the effective coordination of all FP basic components and related assets. The FC, sector and unit commanders must provide clear FP direction and guidance at all levels of command to initiate operations planning and provide consistency in applying FP measures, tasks and activities. Mission specific FP SOPs and directives should specify FP procedures from the identification of threats to the response phase along with, associated task elements, equipment, and infrastructure for FP. The FP organization at battalion, sector and FHQ levels should be Command led and include early warning and control centers, response coordinating officials, quick response forces as well as sustainment and reinforcement elements. There should be interconnections and cooperation between the FP organizations at unit, battalion, FHQ and Mission levels. It is essential that authorities, responsibilities and accountability for FP be clearly articulated at all levels of command

66**. The Force Protection Advisory Group.** The Mission Force Protection Advisory Group (FPAG) is an entity established to coordinate all FP issues. FPAG receives information/intelligence support from the Information Community through the Threat Assessment Group (TAG). The military component is part of the FPAG in each mission. The FPAG consists of the security decision makers, UNDSS, Military component, Police component and other mission elements including the JOC, JMAC and Mission Support.

67**. Force Protection Working Group.**

67.1. Each FHQ should constitute a Force Protection Working Group (FPWG) consisting of FP Focal Points from all units, sector focal points within AOR and Force HQ elements. Similar WGs should be constituted at the Sector level and provide inputs to the FHQ FPWG. The FPWG will be multi-disciplinary and is required to provide assessments and recommendations to the FC and the FPAG on all FP issues as well as monitoring the implementation of required measures. The structure of the FPWG should consist of representatives from deployed units, Operational Effectiveness Inspection Team and any other relevant teams (JMAC, JOC etc.) to ensure reviews and assessments are conducted in the context of the whole Mission. Composition and responsibilities of working group are at Annex F.

67.2 The WG should collate inputs relating to threat, risks, vulnerabilities and measures to be taken throughout the AOR. The FPWG outputs should include alert state recommendation, FP measures to be adopted/reduced and training recommendations.

67.3 FPWG meetings should be conducted monthly while the threat environment, risks, mandates, etc. may be considered in determining the frequency of meetings.

F. ROLES AND RESPONSIBILITIES

68. The FC is responsible to ensure all formed military units develop and implement comprehensive FP measures and activities consistent with identified threats.

G. TERMS AND DEFINITIONS

For the purpose of this guideline, the following terms and definitions shall apply.

Host Country: Host Country is defined as the country in which the United Nations is present and/or conducts its operations at the invitation of the Government.

Hazard: A potential cause of harm resulting from non-deliberate human actions or natural event.

Impact: A rating of the assessed potential harm that an event would have (if it were to occur) on UN operations, activities or mission.

Likelihood: A rating of the assessed potential for a harmful event to effect UN operations, activities or mission.

Proactive Posture: A military posture aimed at preventing an expected or assessed threat before it manifests itself by conducting a military operation or series of operations or by taking various active and passive security measures to prevent an attack on friendly personal or facilities. It is achieved by denying the space and disrupting the capability of opposing violent elements through domination of the area.

Protection: Protection in these guidelines refers to protection of military contingents, United Nations facilities, installations and equipment; and includes ensuring the security and freedom of movement of the United Nations and associated personnel.

Risk: Likelihood of a harmful event occurring and the impact of the event if it were to occur. The combination of impact and likelihood for harm, loss or damage to the UN system from exposure to threats. In these guidelines it includes natural/climatic concerns and hazards.

Risk Management: Risk management involves the planning, preparing, coordinating, rehearsing, and executing of actions to reduce the likelihood (prevention) and/or impact (mitigation) of identified threats and hazards

Threat: A potential cause of harm initiated by deliberate human actions.

United Nations Personnel: Persons engaged or deployed by the Secretary-General of the United Nations as members of the military, police or civilian components of a United Nations operation.

- (Other officials and experts on mission of the United Nations or its specialized agencies such as the International Atomic Energy Agency who are present in an official capacity in the area where a United Nations operation is being conducted)

UNSMS – United Nations Security Management System**:**

Security Risk Management (SRM). A United Nations Security Management System analytical process for systematic determination and implementation of timely and effective approaches for managing the effects of threats to the organization.

Vulnerability: Capable of, or susceptible to being wounded or hurt. Vulnerability is a combination of the attractiveness as a target and the level of deterrence provided by the existing countermeasures.

H. REFERENCES

Normative or superior references

DPO Ref. 2020.01 United Nations Infantry Battalion Manual, January 2020.

DSS-Ref. 20346 United Nations Security Management System Security Policy Manual, October 2017.

DSS United Nations Security Risk Management Manual, March 2020.

DPO Ref. 2016.24 Guidelines on Use of Force by Military Components in Peacekeeping Operations, February 2017.

DPO-DOS Ref. 2019.27 United Nations Manual on Ammunition Management, December 2019.

DPO-DOS Ref. 2015.16 Operational Readiness Assurance and Performance Improvement Policy, December 2015.

DPO Ref. 2018.29 United Nations Guidelines on Operational Readiness Preparation for Troop Contributing Countries in Peacekeeping Mission, November 2018.

DPO-DOS Ref. 2017.18 United Nations IED Threat Mitigation Military and Police Handbook, September 2017.

DPO-DOS Ref. 2019.23 Policy on Authority, Command and Control, October 2019.

DPO Ref. 2019.16 Guidelines on Combined Military and Police Coordination Mechanisms in Peace Operations, September 2019.

DPO Ref. 2019.08 United Nations Military Peacekeeping-Intelligence Handbook, April 2019.

DPO United Nations Military Peacekeeping Glossary of Abbreviations, March 2020.

DPO Ref. 2019.17 The Protection of Civilians in UN Peacekeeping Policy, October 2019.

DPO-DOS Ref. 2016.02 Protection of Civilians: Implementing Guidelines for Military components of United Nations Peacekeeping Missions, February 2016.

DPO-DOS Ref. A/75/121 Manual on Policies and Procedures concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions, 2020.

DPO-DOS Ref. 2010.20 Policy on Training for All United Nations Peacekeeping Personnel, April 2010.

OHCHR Ref. 21844 Human Rights Due Diligence Policy on United Nations support to non-United Nations security forces (A/67/775–S/2013/110).

DPO-DPPA-DOS Guidelines on Improvised Explosive Device (IED) Threat Mitigation in Mission Settings.

UNDSS- United Nations Fire Safety Guidelines-United Nations Security Management System (UNSMS), June 2021

Report of the Secretary-General (A/71/187) of 25 July 2016 'Countering the threat posed by improvised explosive devices.

Lt. Gen. Dos Santos Cruz Report on Improving Security of UN Peacekeepers dated 19 December 2017.

FHQ FRAGO 081/2017 Force Protection dated 17 October 2017.

MILAD MILFAX Needs for Enhanced Force Protection dated 5 January 2018.

I. MONITORING AND COMPLIANCE

69. The Office of Military Affairs will ensure the implementation of this guideline and will propose amendments if and when required.

J. CONTACT

70. DPO/Office of Military Affairs/ Policy and Doctrine Team.

K. HISTORY

71. This is the First Edition of the Guidelines on Force Protection for the Military Component.

APPROVAL SIGNATURE:

Jean-Pierre Lacroix
Under-Secretary General
Department of Peace Operations

DATE OF APPROVAL: 9 September 2021

ANNEX A

PHYSICAL SECURITY

Physical security includes safeguards against destruction, espionage, sabotage and organized crime. Physical security, personnel security, and information security, (including Information and Communications Technology security) are aspects of protective security. The integration of all aspects of protective security achieves a robust security system for bases and camps.

Physical security should be based on the principle of “defence in depth”. Defence in depth is achieved by the creation of layered security measures. Components of the security system shall be designed in sufficient number of layers to make it more difficult to defeat the whole system. All UN bases, camps and units require at least two physical layers of security between personnel or valuable assets and the areas beyond direct UN control, including a system to only allow authorized persons, vehicles and other items to cross these layers (access control).

Physical security measures shall be designed to deter, detect, delay and deny.

> **Deter** – measures that attempt to prevent undesirable action against the premises by influencing the attacker’s decision making.
>
> **Detect** – measures to detect and assess planning, (or actual attempts) by threat actors to penetrate the security perimeter or test the effectiveness of the security systems in place.
>
> **Delay** – physical barriers or measures to restrict movement and to allow time for appropriate response.
>
> **Deny** – the ability to oppose, disperse or negate the effects of an action against the premises, including denying access to information on the layout and contents of the premises. The security system shall be designed to deny identified threat actors the ability to carry out a successful, harmful action.

Physical Security Measures shall include:

1. A perimeter fence: A perimeter fence identifies the boundary of an area requiring security protection. It provides a degree of physical protection and psychological deterrence to intrusion. All UN premises shall have a clearly defined and protected perimeter through which all entry and exits are controlled.

2 Security lighting: Security lighting can offer a high degree of deterrence to a potential intruder in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system.

3. Intrusion Detection Systems (IDS): Perimeter Intrusion Detection Systems (PIDS) may be used on perimeters to enhance the level of security offered by a perimeter fence. PIDS should be used with an alarm verification system.

4. Access Control: The control may be electronic, electro-mechanical, by a guard or physical means. All UN premises shall have an access control system that admits only individuals appropriately cleared and authorized to enter the area.

5. CCTV: Closed Circuit Television is a valuable aid to guards on duty in verifying incidents and PID alarms on large sites or perimeters. The effectiveness of such a system will, however, depend on the suitability of equipment, its installation and monitoring within the control centre.

6. Observation Posts: Forward observation posts should be deployed and equipped with night vision equipment, laser range finders, special weapons and ammunition (as required by a threat assessment).

7. Patrols. Perimeter patrols are a force protection measure and should be deployed to cover areas that cannot be observed from the observation posts.

8. Quick Reaction Force/Team (QRF/T). The QRF is designed for rapid deployment anywhere in the Mission AO and is often under the direct operational control of the FC.

9. Physical Defence Structures. Physical defence structures should include field fortification/bunker protective shelters, hardened buildings, barriers, and stand-off distances. The extent and type depend on identified threats.

10. Fire Detection Equipment. Fire detection equipment should include fire detection and alarm systems, fire suppression systems, fire and smoke compartmentalization. Fire detection units are supported by the Mission.

11. Ammunition Protection. Measures should be taken in line with the UN Manual on Ammunition Management which includes the defence, protection, and safe management of ammunition storage areas. When not in use arms, ammunition and explosives should be stored in armories, ammunition and explosive stores or permanently manned posts that have been approved by UN security staff.

12. Chemical Biological Radiological and Neurological (CBRN) Equipment. CBRN equipment include gas masks, canisters, gloves, detection kits, de-contamination means and suits. CBRN equipment protects personnel from potential CBRN attacks or accidents.

13. Air defence. Air defence includes both active and passive measures. Active air defence involves defensive actions taken to destroy, nullify, or reduce the effectiveness of air and missile attacks. Passive air defence includes other measures to minimize the effectiveness of such attacks through individual and collective protection of the force and critical assets (such as physical defence structures).

ANNEX B

FUNDAMENTAL ELEMENTS OF FORCE PROTECTION

Serial	Elements	Responsibilities
1.	**Security**	**Personnel Security** **Physical Security** **Information Security** **Weapons and Ammunition Security**
2.	**Force Engineering Security**	**Physical Protection** **Improvised Explosive Ordnance Disposal** **Explosive Device Disposal** **Explosive Threats and Hazards Awareness** **Fire Protection** **Post Attack recovery**
3.	**Health**	**Evacuation** **Safety** **Treatment** **Public/Environmental Health** **Disease**
4.	**Air Assets Security**	**Airports/Airstrip/Helipad Security** **Aircraft approach and depart lanes** **Air Facilities/equipment** **Aircraft (including Helicopter, UAS) Security** **Active Air Defense systems**
5.	**CBRN**	**Detection, Identification and Monitoring** **Medical Counter Measures** **Hazard Management**

ANNEX C

THREAT ENVIRONMENT LEVELS

The threat environment is categorized into six levels based on the UN security level system**.**

Minimal Threat Environment. No foreseeable risk of a threat or harm to the organization, its assets, or personnel and the implementation of its mandate. To sustain a minimal threat environment, the following features shall/may exist:

-Well organized structures (Both United Nations and Host Nation).

- No threat identified

-Wide range of security systems or force protection measures protecting UN personnel and assets.

-A range of security measures against the organization or environment that makes attacks or disruption more demanding.

-Mission or environment has sufficient capacity to continue functioning should there be an attack

Threat Scale – 1 or White

Low Threat Environment. An environment in which there is little or non-significant risk of threat or harm to the organization (assets or personnel) and the mandate implementation. If there is a foreseeable threat, it will result in minor disruption. To sustain a low threat environment, the following features shall/may exist:

-Well organized structures (Both United Nations and Host Nation).

- Little or non-significant threat/Limited activities of belligerents

-Wide range of security systems or force protection measures protecting UN personnel and assets.

-A range of security measures against the organization or environment that makes attacks or disruption more demanding.

-Mission or environment has sufficient capacity to continue functioning should there be an attack

Threat Scale – 2 or Green

Moderate Threat Environment. Moderate risk of threat or attack exist in this environment and occur periodically. Threats or attacks against the organization will cause considerable inconvenience to mandate implementation. To mitigate or sustain such environment, the following features could exist:

-Wide range of security system or force protection measures protecting UN personnel and assets.

-A range of security measures against the organization or environment that makes attacks or disruption more demanding.

-Mission or environment has moderate/average capacity to continue functioning should there be a threat or high risk of attacks, replacement of equipment and some injuries to personnel likely.

Threat Scale – 3 or Yellow

Substantial Threat Environment. Strong possibility of threat or attack exists in the environment. The general security environment is hostile with some indications of threats or attacks. The following features could also exist:

- Some movement restriction, minimal loss of freedom of movement for short duration.
- Fluidity in operations (High tempo operation).
- High level security alertness and threat levels.
- Identified belligerent groups/actions.

Threat Scale - 4 or Amber/Orange

High Threat Environment. Very likely/high risk of threat or attack exist in this environment. The organization/environment may experience threat or attacks with little or no prior warning. Belligerent activities are high and have significant impact and inconvenience to mandate implementation. The Mission will sustain damage to vehicles, equipment and infrastructure and peacekeeper casualties and injuries. The following features could also exist:

-Movement restriction.

-Fluidity in operations (High tempo operations).

-Simultaneity in belligerent actions (well organized actions).

-High level of security alertness and threat levels.

-Breakdown of law and order (Anarchy).

-Collapse of state security institutions.

-Terrorist actions.

Threat Scale – 5 or Red

Extreme Threat Environment. Most likely or significant risk of threat or attack exist in this environment. The organization/environment experiences threat or attacks with no prior warning. Belligerent activities are very high and have most critical/noticeable impact and harm to mandate implementation. Mission has no capacity to recover after an attack. The following features could also exist:

-Movement restriction.

-Fluidity in operations (High tempo operations).

-Simultaneity in belligerent actions.

-Terrorist activities.

-High levels of security alertness and threat levels.

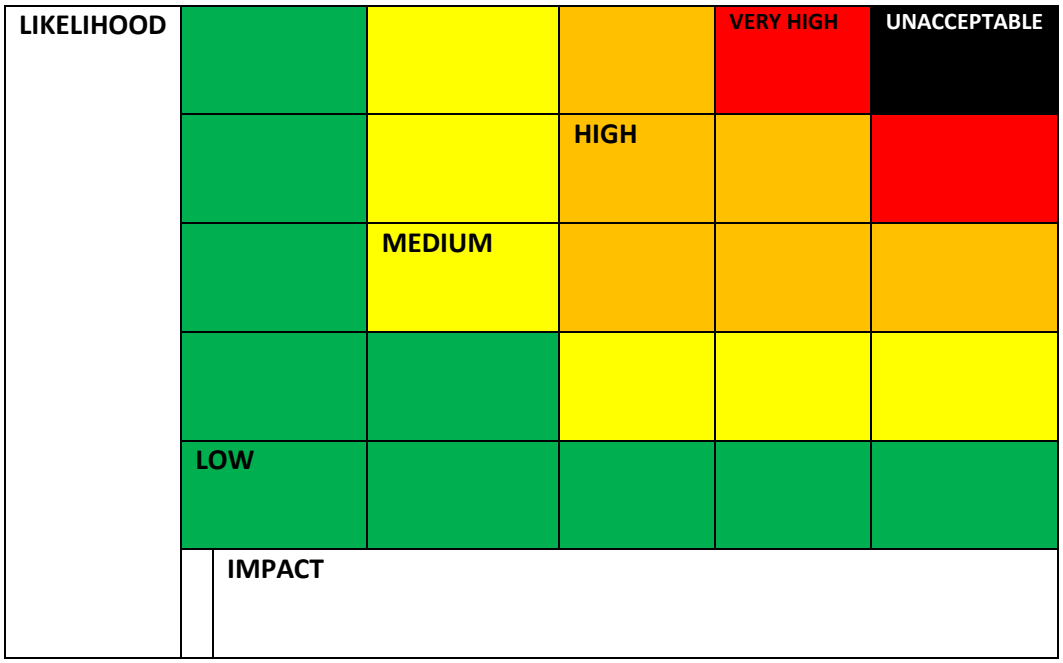
-Breakdown of law and order (Anarchy).

-Collapse of state security institutions.

Threat Scale – 6 or Black

ANNEX D

RISK ANALYSIS MATRIX



Note

- Risk is a combination of likelihood and impact.
- The highest priority risk is assigned to the most likely threat, with the greatest impact.
- Managing risk involves managing likelihood and impact.

ANNEX E

ALERT STATES, DRESS CODES AND VEHICLE MOVEMENT CODES

Alert State	Dress Code	Vehicle Movement Code	Weapon Code
ONE This applies when there is no foreseeable threat or harm to personnel, units or formations.	**Dress Code 0** Full national uniforms with soft hat are to be worn	**VM Code 0** Movement not restricted. Single vehicle movement permitted with single person. Weapon not required.	**WU** Weapons unloaded, no magazine in the weapon, no round in the chamber, magazines readily available.
TWO This applies when there is little or no significant threat or harm.	**Dress Code 0** Full national uniforms with soft hat. Outside military areas, helmet and body armour are to be close at hand.	**VM Code 1** Movement not restricted. Single vehicle movement is permitted with single crew. Weapons on order of local commanders.	**WU** Weapons unloaded, no magazine in the weapon, no round in the chamber, magazines readily available.
THREE This applies when there is minimal threat of attack or harm.	**Dress Code 1** Full national Uniforms with soft hat are to be worn inside military areas. Outside military areas helmet and body armour are to be worn. Personal weapon is to be close at hand	**VM Code 2** Movement not restricted. Single vehicle movement is authorized with minimum of 2 person crew for each vehicle. Outside military areas, military vehicles should be guarded	**WL** Weapons Loaded, magazines in the weapon, no round in the chamber.
FOUR This applies when there is a likely probability of threat of attack or harm. Threats or attacks will cause considerable inconvenience to mandate	**Dress Code 2** Outside military areas full national combat uniform, helmet, body armour, and personal weapon with ammunition are to be worn.	**VM Code 3** Minimize movement. Restrict or reduce movement for specific periods of time, in specific areas or to specific locations as appropriate.	**WL** Weapons Loaded, magazines in the weapon, no round in the chamber.
FIVE	**Dress Code 2**	**VM Code 3**	**WR**

This applies when there is a very likely/high risk of threat, harm or attack.	Outside military areas full national combat uniform, helmet, body armour, and personal weapon with ammunition are to be worn. Inside military areas the above equipment is to be close at hand.	**.** Minimize movement. Restrict or reduce movement for specific periods of time, in specific areas or to specific locations as appropriate. **.** Movement with a minimum of two vehicles. **.** Minimum two-person crew per vehicle. **.** Communication required in at least one vehicle. **.** All personnel are to be armed. **.** Outside military areas, military vehicles should be guarded.	Weapons ready, round in the chamber, weapon on safe.
SIX This applies when there is most likely or significant risk of threat, harm or attack against personnel, units, and facilities.	**Dress Code 3** Full national uniform, body armour, helmet, personal weapon with ammunition are to be worn all the time.	**VM Code 4** **.** Only mission essential movement is permitted. **.** No road movement without armoured escort equipped with appropriate communication. **.** Movement with a minimum of two vehicles, **.** Minimum two person crew per vehicle. **.** All personnel are to be armed. **.** Communication required in all vehicles.	**WR** Weapons ready, round in the chamber, weapon on safe.

Note

Vehicle Movements. The following control measures are to be applied for all vehicle movements:

a. All vehicles are to book out through their designated movement control organization providing destination and estimated arrival time.

b. All vehicles are to confirm arrival to their movement control organization.

c. If personnel have not reported back within 3 hours of ETA, the designated movement control organization is to initiate a search.

d. Random routes should be used whenever possible to avoid predictability.

Road Movement Safety Restrictions:

a. OPEN - No restrictions.

b. RESTRICTED - Only mission essential movements on these roads.

c. CLOSED - No movement on these roads.

ANNEX F

COMPOSITION AND RESPONSIBILITIES OF THE MILITARY FHQ FORCE PROTECTION WORKING GROUP (FPWG)

1. Composition of Force Protection Working Group (FHQ)

- **FCOS**. The FCOS leads the Sub-committee on all FP issues. The FCOS is responsible for initiating, planning, conducting and monitoring all phases of the FP process decisions/recommendations made by the Sub-committee. The FCOS is to present all decisions/recommendations to the FC for approval.

- **Sector/Unit Commanders**. Monitor and establish FP measures coordinated through the FP Sub-committee. Identify specific FP training requirements in sectors/units.

- **DCOS Ops**. The DCOS ops deputizes for the FCOS. The DCOS ops is to advise and support the FCOS in the decision-making process. Monitor the FP Assessment.

- **Chief U-5**. The Chief U-5 shall ensure that FP considerations are incorporated in the Force's OPLAN. Additionally, the U-5 shall coordinate and lead internal evaluation of the Force's FP framework.

- **Chief U-3.** The Chief U-3 shall monitor FP at sector and battalion levels and through the DCOS Ops, advise the FCOS on FP issues.

- **Chief U-2**. The Chief U-2 shall provide analysis of emerging threats and information/ intelligence support to the Sub-committee.
.
- **Operational Effectiveness Inspection Section/Team**. The operational effectiveness section/team shall provide the latest evaluation reports performed by each unit.

- **Force Engineers**. Force Engineers shall advise on FP engineering plans and emplace FP engineering and infrastructure measures to reduce identified risks and mitigate the effects of the threat (mines, unexploded ordnance, environmental effects, natural elements, etc.). These measures should include hardening of facilities; repairing airfields and routes; erecting barriers; providing cover and concealment; determining stand-off distances; route, airfield, and port clearances; mobility and counter mobility measures; support to C-IED activities; as well as coordinating fire protection and supporting EOD activities. Force Engineers shall also provide technical assistance and training as required.

- **Provost Marshal**. The provost marshal shall provide advice and ensure the good conduct, discipline and compliance of military personnel (and where necessary other residents of UN camps/team-sites) with established FP protocols.

- **Logistics.** The U-4, in close coordination with the joint logistics support group (JLSG), should coordinate with the U-3 on FP requirements for logistic forces and facilities, as well as providing the necessary support to satisfy the needs of all FP measures, tasks, and activities

- **Mission Support**. Representatives of relevant mission support components (e.g. Mission Support Center, Engineering and Facility Management.).

- **Medical**. The medical advisor is responsible for advising on health threats and hazards, their probable impacts and the prevention and response measures as required.

- **FHQ Force Protection Cell** (if part of the FHQ structure) -
-
- **JMAC** – TBD.

- **JOC** – TBD.
- Additional members may be included on an ad hoc basis if their expertise of the situation demands it.

2. **Responsibilities of Force Protection Working Group**

Responsibilities shall include:

- Monitor and establish FP measures coordinated through the Force Protection Advisory Group.
- Collate inputs on threats, risks, vulnerabilities and measures across the AOR
- Review and monitor the development of FP plans at the Sector Level and below.
- Review FP issues that arise at the Sector level or below and facilitate the development of adequate mitigation measures.
- Review and make recommendations for adjustment to Alert states to the Force Commander.
- Periodically review training requirements related to Force Protection.
- Monitor and assist Sector FP focal points, subordinate formations and units in the implementation of FP policies and standards.
- Ensure a Force Protection Assessment Team is established in each Sector, which shall compose of experts in the following areas:

    - FP and security operations.
    - Peacekeeping-Intelligence.
    - Infrastructure and engineering.
    - Communications.
    - Medical and Environmental Health.
    - Firepower and Mobility.

- Ensure similar WGs are constituted at the Sector Level.