

UNCLASSIFIED



United Nations
Department of Peace Operations
Ref. 2022.05

Guidelines

Sharing Peacekeeping- Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities

Approved by: Jean-Pierre Lacroix, USG DPO

Effective date: *1 December 2022*

Contact: *DPO/OUSG/PICT*

Review date: *1 December 2024*

DPO GUIDELINES ON SHARING PEACEKEEPING-INTELLIGENCE WITH AND RECEIVING INTELLIGENCE FROM NON-UN AND NON-MISSION UN ENTITIES

Contents:	A. Purpose and Rationale
	B. Scope
	C. Procedures
	- Sharing Peacekeeping-Intelligence
	- Receiving Intelligence
	D. Roles and Responsibilities
	E. Terms and Definitions
	F. References
	G. Monitoring and Compliance
	H. Contact
	I. History

ANNEXURES

- A. Entity Assessment for Sharing – Sample**
 - B. Sharing Risk Assessment – Sample**
 - C. Flowchart of Sharing PKI**
 - D. Entity Assessment for Receipt – Sample**
 - E. Intelligence Receipt Scan– Sample**
 - F. Flowchart of Receiving Intelligence**
-

A. PURPOSE AND RATIONALE

1. These Guidelines expand on paragraphs 10.4. and 11.4. of the Peacekeeping-Intelligence Policy and elaborate on why and how United Nations (UN) peacekeeping missions may share peacekeeping-intelligence (hereinafter “PKI”) products with non-UN and non-mission UN entities, and receive intelligence products from non-UN entities. They articulate the parameters by which such sharing and receiving can be conducted, and also outline a recommended decision-making structure for this purpose. These Guidelines only apply to the sharing of PKI with and receipt of intelligence products from non-UN and non-mission UN entities by UN peacekeeping missions.
2. Non-UN entities may include, for example, the Ministry of Foreign Affairs of the Host State of a peacekeeping mission, regional organizations or missions thereof, non-governmental organizations, and entities within individual Member States, including troop- and police-contributing countries (ex. Armed Forces). Non-mission UN entities may include, for example, UN agencies, funds and programmes, as well as certain Secretariat entities in a non-integrated mission setting. UN Headquarters entities, such as DPO, are not included among such entities for the purpose of these Guidelines.
3. The DPKO-DFS Policy on Peacekeeping Intelligence was promulgated in May 2017, and updated as the DPO Policy on Peacekeeping-Intelligence (hereinafter “the Policy”),

effective 1 May 2019. The Policy, under paragraphs 11.4. titled “Peacekeeping-intelligence sharing with non-mission and non-United Nations entities,” provides an outline of procedures pertaining to the sharing of peacekeeping-intelligence with such entities. The Policy, under 10.4., refers to the possible receipt of intelligence from external parties.¹ These Guidelines are designed to provide missions with additional, more detailed guidance.

4. In liaising with any such external party for the purpose of sharing and receipt, mission personnel shall fully observe and act consistently with the mission’s mandate and all principles, rules and obligations of the Organization, including with regard to the promotion and protection of international human rights laws and norms. The absence of appropriately detailed guidance or the non-compliance thereof could result in actions that may lead to the endangerment of mission personnel, the local population, and those from whom information was acquired, as well as negatively impact the reputation of the Organization.

B. SCOPE

5. These Guidelines apply solely to missions that wish or need to share PKI with, or that receive intelligence from, non-UN and/or non-mission UN entities. Compliance with these Guidelines is mandatory for relevant components of such missions. The Head of Mission, in particular, as well as other senior mission leadership, play a key role in ensuring their compliance.
6. These Guidelines apply to the sharing of PKI and receipt of intelligence only; for the exchange of sensitive information that is not considered intelligence or PKI, and all handling related thereto, the existing relevant guidance will continue to apply.
7. For the sharing of PKI and receipt of intelligence, these Guidelines apply to all methods thereon, including PKI that is shared and intelligence that is received orally or via other informal means.

C. PROCEDURES

- These Guidelines comprise two sections. The first section outlines relevant procedures in relation to the sharing of PKI, while the second section explains those regarding the receipt of intelligence.
- The first section is further divided into two sub-sections: (1) Sharing PKI with non-UN entities; and (2) Sharing PKI with non-mission UN entities.
- In principle, intelligence/PKI is categorized as either strategic or operational/tactical, depending on where the initial direction came from. Strategic intelligence/PKI would have been produced in response to a direction at the HoM level, while for operational/tactical intelligence/PKI, the direction would have come from the sub-HQ/field office level. Please see F. Terms and Definitions for further

¹ Both non-UN entities and non-mission UN entities are considered such parties for the purpose of these Guidelines.

detail on each.

- Throughout both the sharing and receiving processes, Information Management Focal Points or other authorized and trained personnel (hereinafter referred to collectively as “IM FP” or “IM FPs” (Focal Point/s)) should play a central role in the facilitation and coordination of the sharing of PKI and receipt of intelligence.² Preferably, IM FPs should be situated in the Office of the Mission Chief of Staff or a similar, cross-cutting or central office that is not directly connected to a specific component or office. In some missions, the IM function may sit within the JMAC/ analytical unit, or the JOC.
- The responsibilities for IM FPs should include the following:
 - a. Advising relevant personnel on the sanitization of PKI prior to sharing, as appropriate.³
 - b. Liaising with the relevant entity(s) regarding all assessments and scans,⁴ which are a structured way to assess and mitigate the risks accompanying the sharing of PKI or receipt of intelligence. Samples of all four are included as annexes.
 - c. The registration of shared PKI products and intelligence products received in official UN information management systems, including verbally shared PKI and received intelligence.
 - d. The maintenance of registers and periodic revisions thereof to identify any trends over time.
IM FPs should consult with the Senior Legal Advisor or other legal colleagues of the mission when they have concerns that may have legal ramifications related to their work.
- Depending on the need and resources available, PKI entities may also wish to appoint component-level IM FPs. Component-level IM FPs are expected to work closely together with (mission-level) IM FPs.
- Registers are a key and requisite tool in the management of both shared PKI and received intelligence.
 - a. **All missions should establish and maintain a central registry where relevant information on a shared PKI or received intelligence product, such as the time, date, its sensitivity marking, and with/from whom and how a product was shared/received, is systematically recorded.** Additional information, such as the results from the Sharing Risk Assessment or Intelligence Receipt Scan, as well as whether any action was taken, should also be recorded.

² The experience and educational standards for an IM FP should be comparable to that of a P3 Information Management Officer (https://iseek.un.org/departamental_page/gjp-information-management-0). Trainings that would complement the necessary experience and educational requirements as outlined above are available here: https://iseek.un.org/system/files/data_and_analytics_curriculum.pdf. As the Secretariat develops further guidance in this field, more trainings can be expected to become available.

³ Sanitization refers to the process of removing sensitive information from a document so that it may be distributed to a broader audience, including the removal of sensitive details of information provided that could trace back to a source or asset and expose them, or make identifiable any possible witnesses or victims related to the information provided.

⁴ There is a total of four: (1) Entity Assessment for Sharing; (2) Sharing Risk Assessment; (3) Entity Assessment for Receipt; and (4) Intelligence Receipt Scan.

- b. The procedures on the recording of information regarding shared PKI/received intelligence shall be detailed in the Mission PKI Support Plan (MISP).
- c. All registers shall be securely managed, and accessible only to relevant personnel. IM FPs shall be responsible for the day-to-day management thereof.
- d. All registers shall be fully accessible to OIOS and other relevant oversight mechanisms as necessary.

8. Sharing of Peacekeeping-Intelligence with Non-UN and Non-Mission UN Entities

- **Sharing Authority**
 - a. The authority to share, which lies with the Head of Mission (HoM), should be appropriately delegated. When a decision is made to delegate, this shall be clearly indicated in the MISP. HoMs may wish to delegate this authority to different personnel depending on the security classification level of a PKI product, as well as to whom the product will be shared. HoMs shall ensure that their delegated authority is fully informed as to the principles and parameters governing the sharing of PKI with non-UN and non-mission UN entities.
 - b. The specific processes of the delegation of authority according to recipient,⁵ and the security classification level and nature of the product (strategic or operational/tactical) should be determined by each mission to best fit their respective circumstances. For the sharing of strategic PKI, it is recommended that authority be delegated to the Chair of the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM).

8.1. *Sharing Peacekeeping-Intelligence with Non-UN Entities*

- 8.1.1. Prior to a mission sharing any PKI with a non-UN entity, an Entity Assessment for Sharing and a Sharing Risk Assessment shall be conducted to evaluate the possible harm that the sharing of such PKI may inflict on the mission or its mandate.⁶
- 8.1.2. An Entity Assessment for Sharing is conducted on the entity with which PKI will be shared. It comprises two parts: (1) an overview of relevant information regarding the entity; and (2) a human rights assessment of the entity. Under (1), missions shall ascertain the scope of the particular entity with which they intend to share, so that there is no ambiguity with regard to the application of the “originator control” principle (ref: 8.1.5.). For non-UN security forces, as defined in the Human rights due diligence policy (HRDDP), including civilian authorities directly responsible for such forces, the human rights assessment portion of the Assessment should be the HRDDP Risk Assessment,⁷ while for civilian non-security force

⁵ Sharing a PKI product with a non-mission UN entity, a non-UN entity, including a non-UN security force, for example.

⁶ An Entity Assessment for Sharing needs to be conducted only when one is not already available or is considered not up to date (ref. 8.1.2.3.).

⁷ A sample of this assessment is available in Annex 1 of the [Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces Guidance Note \(2015\)](#), and detailed guidance on how to conduct an assessment is available on pp. 18-24 of the same document. Where the UN entity has an SOP for the implementation of the HRDDP, the HRDDP risk assessment shall be conducted in accordance with the procedure set out in the SOP.

entities⁸, the HRDDP Risk Assessment should be adapted according to the mission's judgment. Please see Annex A for an example of an Entity Assessment for Sharing.

- 8.1.2.1. Missions should determine which component/unit is best positioned to conduct part (1) based on the nature of the PKI (strategic or operational/tactical), and who conducted the analysis of the acquired information. Part (2) should be conducted by the human rights component of the mission in consultation with other relevant components and follow specific procedures in place to conduct HRDDP Risk Assessments, as relevant. If a mission does not have a human rights component, they should reach out to the Office of the High Commissioner for Human Rights (OHCHR) through their human rights focal point.
- 8.1.2.2. The HRDDP Risk Assessment or adapted HRDDP Risk Assessment (as applicable) should include, as necessary, mitigation measures aimed at reducing risks prior to any sharing taking place. The sharing entity shall ensure that the mitigation measures are implemented by the information-receiving entity.
- 8.1.2.3. Once conducted, missions should regularly review and update Entity Assessments for Sharing, so that they may be used in subsequent instances of sharing with the same entities. Active monitoring of relevant developments or incidents is particularly important for up-to-date Entity Assessments for Sharing of non-UN security forces. At a minimum, Assessments should be reviewed after a set period of time that is determined by the mission (ex. at least every three months).
- 8.1.3. A Sharing Risk Assessment is conducted on the PKI product that is to be shared. Unlike Entity Assessments for Sharing, Sharing Risk Assessments should be conducted for each product that will be shared (with the exception of regularly shared PKI products – see 8.1.8.). Please see Annex B for an example of a Sharing Risk Assessment.
 - 8.1.3.1. Missions should determine which component/unit is best positioned to conduct the Sharing Risk Assessment based on the nature of the PKI (strategic or operational/tactical), and who conducted the analysis of the acquired information. The human rights component should be consulted in this process as necessary.
 - 8.1.3.2. If sharing operational/tactical PKI with non-UN entities, the office/unit that originally acquired the information shall be

⁸ With the exception of national civilian authorities directly responsible for the management, administration or command and control of non-UN security forces, to whom the HRDDP risk assessment should be conducted as per policy.

consulted, and must support its sharing.

- 8.1.4. The sharing of PKI can take place once the mission conducts both the Entity Assessment for Sharing and Sharing Risk Assessment, and concludes that the risk of doing so would be acceptable.
- 8.1.5. When sharing PKI, the following conditions shall be transmitted to and accepted in writing by the non-UN entity:
- Recognition of and strict adherence to the “originator control” principle. **Should the entity wish to share a PKI product with another entity, it shall first obtain the explicit written approval of the mission to do so.**
 - In line with the principles of PKI,⁹ agreement by the entity that any subsequent use of shared PKI products will:
 - Be strictly limited to activities or operations that pertain to the safety and security of UN personnel, situational awareness, and the protection of civilians; or
 - Be applied to a more limited scope than that above, articulated by the mission.
 - Agreement that shared PKI products will not be used to instigate or facilitate the commission of human rights violations, breaches of international humanitarian law, or any other international crimes.
 - Agreement that shared PKI products will maintain their security marking.¹⁰
 - Agreement that classified PKI products will be handled and secured at the same standards as those for intelligence products at the equivalent security classification level of the receiving entity, or at a standard otherwise agreeable to the mission.
- 8.1.6. Missions may also decide to partially share PKI. In such cases, all conditions above must still be met.
- 8.1.7. Should there be PKI products that require urgent sharing, steps 8.1.1.- 8.1.4. shall still be followed; in these instances, they should be implemented by the relevant personnel **as a matter of utmost priority**. Missions may wish to have procedures in place to alert relevant personnel as to its urgency, and to make clear the need to prioritize its processing, including time limits. All conditions listed under 8.1.5. shall continue to apply in the sharing of such PKI products.
- 8.1.8. Should there be PKI products that are shared on a regular basis, missions may wish to set up a standardized clearance procedure for this purpose. One such option may be to create and maintain a list of pre-authorized entities to whom such products can be shared. Even in these cases, each product that is shared shall be forwarded to the IM FP to ensure its appropriate registration in the registry, and the list should be periodically reviewed (ex. at least every three months).

⁹ See 9.4. Areas of application under the Policy on Peacekeeping-Intelligence.

¹⁰ Classification levels accorded to PKI products should be in line with ST/SGB/2007/6 on Information sensitivity, classification and handling, and any other relevant UN guidelines/SOPs.

- 8.1.9. Should PKI have been shared via informal means (verbally, for example), personnel should report as much information as possible to an IM FP, for appropriate registration in the register.
- 8.1.10. Should there be a breach of the conditions specified in para. 8.1.5, or substantial suspicion thereof, further sharing of PKI shall be halted pending an internal mission investigation and in line with the HRDDP; the resumption thereof shall be conditional on positive conclusions of the investigation, as well as a re-assessment of the risks and benefits of a continued intelligence/PKI relationship with the entity. If the sharing of PKI is resumed, the mission may wish to do so at a lower level and/or on a case-by-case basis for an initial period of time.
- 8.1.11. All decisions to share PKI shall be taken on a case-by-case basis, in line with these Guidelines and any related guidance issued by missions. The results of both Assessments should also be carefully considered. Further, missions should weigh their “need to share” PKI with the counterpart entity’s “need to know,” as well as the following criteria: (1) whether the entity is operating in or in close proximity to the Area of Operations of the mission; (2) whether the entity has an organizational structure that is able to adjust its operations or activities based on newly received information; and (3) whether the entity is operating with a mandate in line with that of the mission. For non-UN security forces, their track record for operations in compliance with the HRDDP should also be given strong consideration.
- 8.1.12. Any part of the PKI product that, in combination with other data sources, could be traced back to any sources or assets, or make identifiable possible witnesses or victims, shall be appropriately sanitized prior to any sharing.¹¹ IM FPs should advise on this process as needed.
- 8.1.13. A flowchart of the overall process is available at Annex C.

8.2. *Sharing Peacekeeping-Intelligence with Non-Mission UN Entities*

- 8.2.1. PKI should be shared with non-mission UN entities as follows:
- Strategic PKI should be shared with the Head of Office or equivalent of the entity.
 - Operational/tactical PKI should be shared with the senior-most DSS official stationed at the duty station and the Designated Official for security. In integrated missions, the same process should also be followed.¹²
 - If the PKI includes Protection of Civilians (PoC) threats, the receiving component shall additionally alert the senior-most manager responsible for PoC, and/or the representative designated as such.

¹¹ Further, in line with ST/SGB/2007/6, no information should be disclosed that would: (i) present a risk to the safety of any individual, (ii) violate a duty of confidentiality which the United Nations owes to a third party, (iii) compromise the confidentiality of the Organization’s internal decision-making process, or (iv) impede the effective functioning of current or future operations of the United Nations.

¹² DSS/DO for security should then share with relevant non-mission UN entities following these Guidelines.

The above officials shall then share the PKI with relevant personnel, according to the officials' "need to share" and the personnel's "need to know."

- 8.2.2. All sharing of PKI to non-mission UN entities shall be systematically recorded in the relevant registry by the IM FP in the same manner as when sharing with non-UN entities.
- 8.2.3. **The "originator control" principle shall also apply when PKI is shared with non-mission UN entities.** Namely, should the entity wish to share a PKI product with another entity, it shall first obtain the explicit written approval of the mission to do so.
- 8.2.4. In line with the principles of PKI,¹³ agreement by the entity that any subsequent use of shared PKI products will:
 - Be strictly limited to activities or operations that pertain to the safety and security of UN personnel, situational awareness, and the protection of civilians; or
 - Be applied to a more limited scope than that above, articulated by the mission.
- 8.2.5. Any part of the PKI product that, in combination with other data sources, could be traced back to any sources or assets, or make identifiable possible witnesses or victims, shall be appropriately sanitized prior to any sharing. IM FPs should advise on this process as needed.
- 8.2.6. The security marking of PKI products should be maintained, and handled and secured appropriately according to their security classification level.

9. Receiving Intelligence from Non-UN Entities

- Receiving Authority
 - a. Once verified, the authority to determine how received intelligence should be disseminated within the mission should be appropriately assigned depending on the security classification level of an intelligence product, from whom the product was received, as well as the nature of the product (strategic, operational/tactical).
 - b. The specific processes of the assignment of authority according to the entity that shared the product,¹⁴ and the security classification level and nature of the product (strategic or operational/tactical) should be determined by each mission to best fit their respective circumstances. For strategic intelligence, it is recommended that authority be assigned to the Chair of the MICM.
- 9.1. Once an intelligence product is received, determination should be made as to whether it is regarding a clear and imminent threat to United Nations personnel and/or civilians.

¹³ See 9.4. Areas of application under the Policy on Peacekeeping-Intelligence.

¹⁴ Receiving a product from a non-mission UN entity, a non-UN entity, or a non-UN security force, for example.

- 9.2. Steps 9.4.-9.7. shall still be followed upon the receipt of such intelligence; in these instances, they should be implemented by the relevant personnel **as a matter of utmost priority**. Missions may wish to have procedures in place to alert relevant personnel upon the receipt of such intelligence, and to make clear the need to prioritize its processing, including time limits.
- 9.3. The receiving component shall also alert the FC and/or Police Commissioner, IM FP(s), and DSS as to the receipt of such intelligence, so that they may prepare to receive the results of the Entity Assessment for Receipt and Intelligence Receipt Scan, and determine whether it should be forwarded to the HoM. If the intelligence includes PoC threats, the receiving component shall additionally alert the senior-most manager responsible for PoC, and/or the representative so designated by the mission.
- 9.4. Once an intelligence product is received, an Entity Assessment for Receipt and an Intelligence Receipt Scan shall be conducted.¹⁵
- 9.5. An Entity Assessment for Receipt, conducted on the entity from which intelligence was received, comprises two parts: (1) an overview of relevant information regarding the entity; and (2) a human rights scan of the entity. Please see Annex D for an example of an Entity Assessment for Receipt.
- 9.5.1. In principle, the component/unit that received the intelligence should conduct part (1) unless the mission determines that another component/unit is better placed to provide the overview. Part (2) should be conducted by the mission human rights component in consultation with other relevant components and follow specific procedures in place to conduct HRDDP Risk Assessments, as relevant.
- 9.5.2. Once conducted, missions should regularly review and update Entity Assessments for Receipt, so that they may be used in subsequent instances of receipt from the same entities. Active monitoring of relevant developments or incidents is particularly important for up-to-date Entity Assessments for Receipt of non-UN security forces. At a minimum, Assessments should be reviewed after a set period of time that is determined by the mission (ex. every three months).
- 9.6. An Intelligence Receipt Scan is conducted on the intelligence product that has been received. Unlike Entity Assessments for Receipt, Intelligence Receipt Scans should be conducted for each product that is received (with the exception of regularly received intelligence products – see 9.10.). Please see Annex E for an example of an Intelligence Receipt Scan.
- 9.6.1. In principle, the component/unit that received the intelligence should conduct the Intelligence Receipt Scan, unless the mission determines otherwise. The human rights component should also be consulted in this process.

¹⁵ An Entity Assessment for Receipt needs to be conducted only when one is not already available or is considered not up to date (ref. 9.5.2.).

- 9.7. Once the Entity Assessment for Receipt and Intelligence Receipt Scan are conducted, and the intelligence product is cleared for mission consumption, the competent authority should determine how it should be disseminated within the mission, depending on the need to know of personnel. All decisions to disseminate and utilize received intelligence products shall be taken on a case-by-case basis, in line with these Guidelines and any related guidance issued by missions.
- 9.8. When receiving intelligence, missions should, in principle, adhere to the following:
- The “originator control” principle. Should the mission wish to share an intelligence product with another entity, it shall first obtain the explicit written approval of the entity from which the intelligence was received.
 - Handle and secure the received intelligence at the same standards as those for PKI at the equivalent security classification level.¹⁶
- Should the entity sharing the intelligence outline specific handling and safeguarding standards, the mission shall ensure that they have the resources and capacity available to do so prior to receiving the intelligence.
- 9.9. Further, the Head of Mission should formally communicate to counterparts that the United Nations will not receive intelligence obtained under torture or by way of other grave violations. If there is a real risk that certain intelligence products have been obtained by way of torture or other grave violations of international human rights or humanitarian law, missions shall neither accept nor solicit such products. The Human Right Component should be immediately informed.
- 9.10. For an entity from which the mission receives intelligence products, especially operational/tactical intelligence products, on a regular basis, the mission may wish to set up a standardized clearance procedure for this purpose. One such option may be to create and maintain a list of pre-authorized entities from which such intelligence products can be received. Even in these cases, each product that is received shall be forwarded to the IMO to ensure its appropriate registration in the registry, and the list should be periodically reviewed (ex. at least every three months).
- 9.11. Should intelligence have been received via informal means (verbally, for example), personnel should report the necessary information to an IM FP, for appropriate registration in the register.
- 9.12. Should the entity that shared the intelligence be deemed untrustworthy, or if the Intelligence Receipt Scan identifies any red flags as determined by the mission, the following additional measures should be taken:
- Increased attention should be paid in the cross-referencing of the particular product with other intelligence, PKI, or information; and
 - If the product is disseminated, it should be done so with a clear flagging of potential issues.
- IMOs shall note this outcome in the registry to enable the tracking of such trends over time.

¹⁶ Such standards should be in line with ST/SGB/2007/6 on Information sensitivity, classification and handling and any other relevant UN guidelines/SOPs.

- 9.13. The following additional points should be duly considered upon receipt of an intelligence product, both strategic and operational/tactical, from non-UN entities:
- While Entity Assessments for Receipt and Intelligence Receipt Scans are conducted, all relevant personnel are nonetheless reminded to carefully scrutinize every intelligence product that they have access to, as there is always a possibility that some details may have been missed or purposefully misrepresented.
 - All received intelligence products shall be used in conjunction with other intelligence and PKI products, as well as other information available to the mission; they shall never be the sole determining source for any action or decision to be taken by the mission.
 - To ascertain the accuracy and trustworthiness of received intelligence, IMOs should actively maintain and regularly review the central registry. If a pattern of doubtful intelligence from a particular entity emerges, that should be duly recorded in the registry, and acted upon as necessary.
 - The above rules and procedures shall also be applied to the handling of intelligence products received from non-mission UN entities but that originate from a non-UN entity.
- 9.14. A flowchart of the overall process is available at Annex F.
-

E. ROLES AND RESPONSIBILITIES

- Head of Mission (HoM)
The HoM is responsible for the overall implementation of these Guidelines, and ensuring that all mission components are fully informed on the processes thereof. The HoM may decide to delegate the releasing authority for the sharing of PKI products. They are required to take immediate action upon receipt of any intelligence that is brought to their attention regarding any imminent threats to the United Nations and/or civilians.
- Chair of Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)
The Chair of the MICM is recommended to be responsible for determining whether a strategic PKI product can be shared with a non-mission entity, as well as to whom a strategic intelligence product that was received from a non-mission entity should be disseminated.
- Human Rights Component
The mission Human Rights Component is responsible for contributing human rights information to all relevant assessments and scans in both the sharing of PKI and receipt of intelligence processes. It will also conduct the HRDDP risk assessments for the assessments set out in paragraphs 8.1.2 and 8.1.3. When there is no Human Rights Component in the mission, OHCHR should be consulted on the record.
- Information Management Focal Point (IM FP)
IM FPs are responsible for registering all PKI products that are shared and intelligence products that are received in a central registry. They are also responsible for the safekeeping of all PKI and intelligence products, along with their scans, and to generally facilitate the internal processes articulated in these Guidelines regarding the sharing of PKI or receipt of intelligence.

- Legal Office in mission
The Legal Office ensures that any documents signed in relation to, for example, the receipt of intelligence, as well as any operational guidance developed subsequent to these Guidelines, are in accordance with the UN Charter, basic principles of peacekeeping, the mandate of the mission, and other relevant rules and regulations pertaining to PKI.
- Participating mission personnel
Each mission personnel who participates in either the process of receiving intelligence from, or sharing PKI with, external entities, is required to adhere to or ensure adherence to these Guidelines, as well as relevant operational guidance.

F. TERMS AND DEFINITIONS

- Mission Peacekeeping-Intelligence Coordination Mechanism (MICM): A mechanism established within the mission to direct and oversee its peacekeeping-intelligence cycle. The Mechanism should comprise the participating mission entities responsible for the acquisition, collation, and analysis of information, with the role of meeting the objectives of peacekeeping-intelligence activities in the mission, i.e., the JMAC, relevant functions in the Force and Police Components, and UNDSS. The JOC should also be a permanent member of the Mechanism, given its role in providing integrated situational awareness. Other mission sections, such as the Legal Office of the mission, the Civil Affairs Division, or the Human Rights Component, may be invited to participate on a permanent or *ad hoc* basis.
- Operational or Tactical Intelligence/PKI: Intelligence or PKI that has been produced in response to a direction given at the operational or tactical level, and whose objective is to inform the decision-making for operations or missions conducted at sub-HQ level within a mission. Tends to be more time-sensitive and dynamic in nature compared to strategic intelligence/PKI, and its geographic scope more limited. Products that are routinely shared between a mission and an external entity would typically fall under this category.
- Peacekeeping-Intelligence (PKI): See para. 9 of the Policy on Peacekeeping-Intelligence for the Principles of Peacekeeping-Intelligence.
- Strategic Intelligence/PKI: Intelligence or PKI that has been produced in response to a direction given by or on behalf of the HoM, and whose objective is to inform the decision-making of the HoM and other senior mission leadership. Products will have a medium- to longer-term outlook, and their geographic scope would typically cover the entire mission area and also beyond.

G. REFERENCES

Normative or superior references

- DPO Policy on Peacekeeping-Intelligence (2019)

Related procedures or guidelines

- Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces (HRDDP) (2011)
- Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces Guidance Note (2015)
- Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions (2016)
- Joint Mission Analysis Centre Field Handbook (2018)
- Military Peacekeeping-Intelligence Handbook (2019)
- OICT SOP on Sharing Information with External Partners (2020)
- Policy on Joint Mission Analysis Centres (2020)
- Secretary-General's Bulletin on Information Sensitivity, Classification and Handling (2007)

H. MONITORING AND COMPLIANCE

8. Within missions, the Head of Mission is accountable for their mission's compliance with these Guidelines, and shall establish mechanisms or processes to enable effective monitoring of compliance. While all mission personnel participating in the peacekeeping-intelligence system are accountable through their chains of management/command for compliance with these guidelines, the mission Chief of Staff, Head of the Legal Office, and Information Management Officer(s) each hold key responsibilities for its effective execution. Regular evaluations of the implementation of these Guidelines may be conducted to assess the degree of compliance therewith.

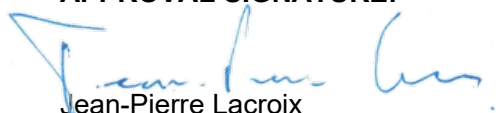
I. CONTACT

9. The contact for these guidelines is the Peacekeeping-Intelligence Coordination Team (PICT), Office of the Under-Secretary-General for Peace Operations, DPO.

J. HISTORY

10. This is the first iteration of these Guidelines.

APPROVAL SIGNATURE:


 Jean-Pierre Lacroix
 Under-Secretary-General
 for Peace Operations

DATE OF APPROVAL: 11 November 2022

ANNEX A: ENTITY ASSESSMENT FOR SHARING (per entity) – SAMPLE

PART 1: Overview of Relevant Information on Entity

- Information regarding non-UN entity (Organization, department/unit, point(s) of contact, positions, contact details etc)
- Suggested questions:
 - What is the entity's mandate?
 - Is the entity's mandate compatible with the mission's mandate?

PART 2: Human Rights Risk Assessment¹⁷

- A template of the HRDDP Risk Assessment is available at Annex 1. of the Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces Guidance Note (2015). Detailed guidance on how to conduct an assessment is available on pp. 18-24 of the same document.
- In line with para. 11.4.4. of the Policy, when sharing PKI with non-UN security forces, including civilian authorities directly responsible for such forces, the HRDDP Risk Assessment should be conducted a priori by the Human Rights Component or by OHCHR where there is no Human Rights Component. For civilian entities, missions should adapt the HRDDP Risk Assessment as they deem appropriate, except national civilian authorities directly responsible for the management, administration or command or control of non-UN security forces, for whom the HRDDP risk assessment should be conducted as per the policy.

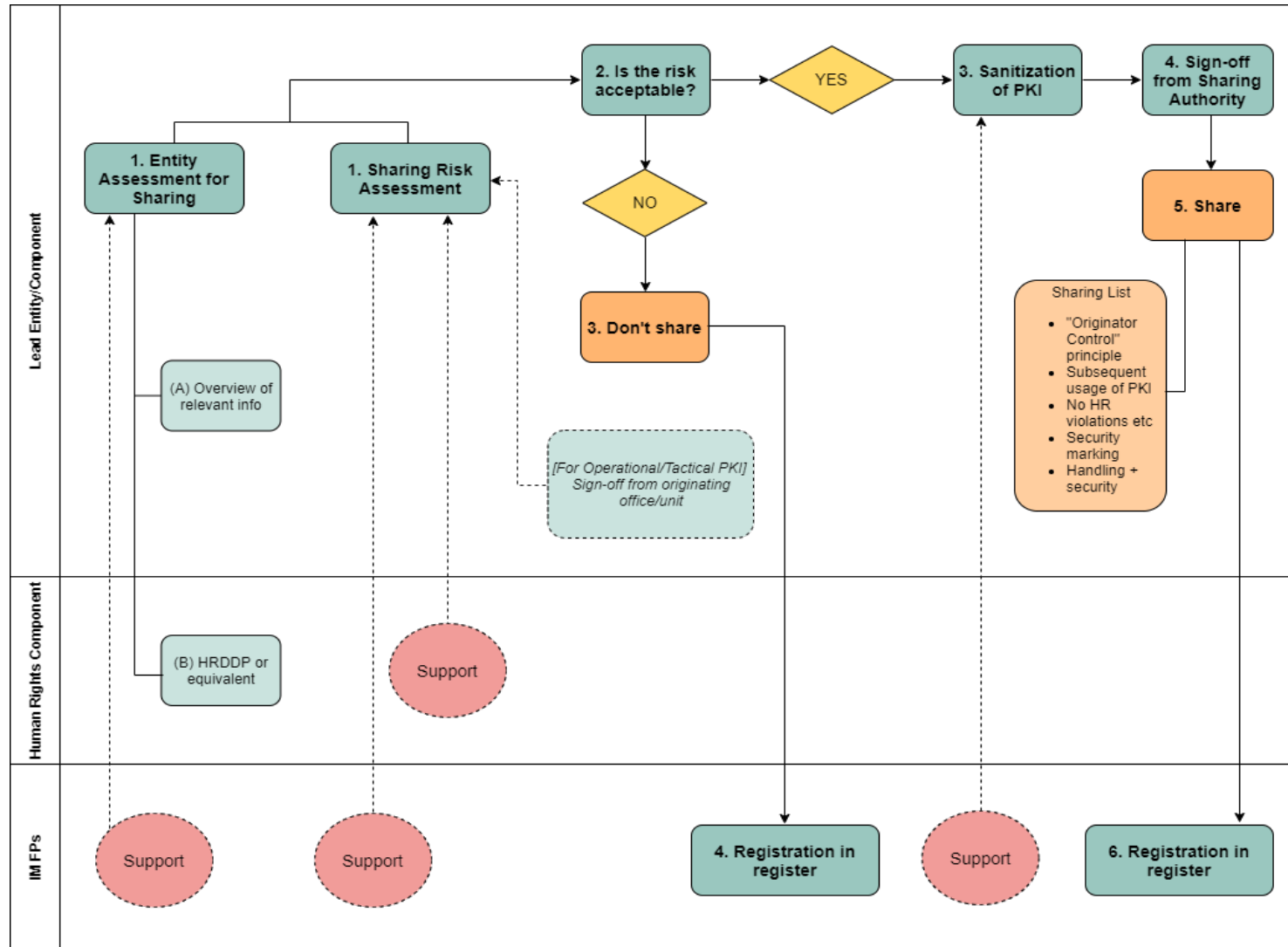
¹⁷ If a particular sub-component of an entity is assessed to be unacceptable to share PKI with, missions may wish to consider making the sharing of a particular PKI product on the condition that it not be shared with that sub-component.

ANNEX B: SHARING RISK ASSESSMENT (per PKI product) – SAMPLE

Suggested questions:

- Is the sharing of this PKI product in line with the mission's mandate?
- Is the sharing of this PKI product in line with the UN Charter, UN rules and regulations, and any bilateral or multilateral arrangements or agreements applicable to [mission name]?
- Has the intelligence/peacekeeping-intelligence product been "sanitized" of any data/information that, in combination with other data sources, could trace back to a source/asset and expose them, or make identifiable any possible witnesses/victims related to the information provided?
- Has the office that originally acquired the information been consulted and agreed to its sharing?
- What can the entity reasonably be expected to do with the PKI product?
- Have there been any issues related to previous instances of sharing PKI with this entity?
- Can the sharing of this PKI product to this recipient reasonably be expected to not cause harm to the UN or, [mission name], its personnel, or its mandate?
- Are there substantial grounds to believe that the PKI being shared may be used to instigate or facilitate the commission of human rights violations, breaches of international humanitarian law, or other international crimes?
- What is the UN classification level of the PKI product?
- Does the entity possess the resources and capacity necessary to handle and secure classified PKI products at the same standards as those for their intelligence products at the equivalent security classification level, or at a standard otherwise agreeable to the mission?

ANNEX C: FLOWCHART OF SHARING PKI



ANNEX D: ENTITY ASSESSMENT FOR RECEIPT (per entity) – SAMPLE

PART 1: Overview of Relevant Information on Entity

- Information regarding entity (Organization, department/unit, point(s) of contact, positions, contact details etc)
- Suggested questions:
 - What is the mandate of the entity?
 - How is the entity involved in the current situation?
 - What are the possible interests and motivations of the entity as it relates to the current situation?
 - Why does the entity want to share intelligence with [mission name]?
 - Has the entity indicated an action that it expects the UN to take in connection with the intelligence they have shared?
- All entities from which intelligence is received should be graded for reliability per the table below.

Table: Reliability Rating of Entity

Entity Reliability		
Rating	Evaluation	Observations
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid intelligence most of the time
C	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid intelligence in the past
D	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid intelligence
E	Cannot Be Judged	No basis exists for evaluating the reliability of the source

PART 2: Human Rights Scan of Entity

- What is the human rights record of the entity (compliance/non-compliance with international humanitarian, human rights, and refugee law)?
- Does the entity have any specific record of “grave violations” of international humanitarian, human rights or refugee law as defined under para. 12 of the HRDDP? (hereinafter “grave violations”)¹⁸
- Is the entity known or suspected to arbitrarily detain personnel, from whom information may have been acquired?
- Is the entity known or suspected to use techniques to question detainees that are not in accordance with international humanitarian, human rights, and refugee law?
- Does the entity have appropriate and effective oversight and disciplinary mechanisms for human rights violations?
- Does the entity have known biases towards specific groups, such as ethnic/religious minorities, women, youth, political groups, persons with disabilities, and LGBTQIA+?

¹⁸ The duration of the record under consideration should be for as long as the mission considers relevant to anticipate possible future behavior.

ANNEX E: INTELLIGENCE RECEIPT SCAN (per intelligence product) – SAMPLE

Suggested questions:

- Does the received product contain intelligence concerning an imminent threat to United Nations personnel and/or civilians?
- Is the received intelligence strategic or operational/tactical?
- Is there reason to believe that the intelligence product received utilized information obtained through “grave violations”?
- Why was the intelligence product shared?
- Is there reason to believe that the intelligence product received may serve political purposes?
- What is the security classification level of the intelligence product?

The credibility of the intelligence received should be graded for reliability per the table below.

Table: Rating of Received Intelligence

Credibility of Intelligence		
Rating	Evaluation	Observations
1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information/intelligence/PKI on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information/intelligence/PKI on the subject
3	Doubtfully True	Not confirmed; possible but not logical; no other information/intelligence/PKI on the subject
4	Improbable	Not confirmed; not logical in itself; contradicted by other information/intelligence/PKI on the subject
5	Cannot Be Judged	No basis exists for evaluating the validity of the information/intelligence/PKI

ANNEX F: FLOWCHART OF RECEIVING INTELLIGENCE

