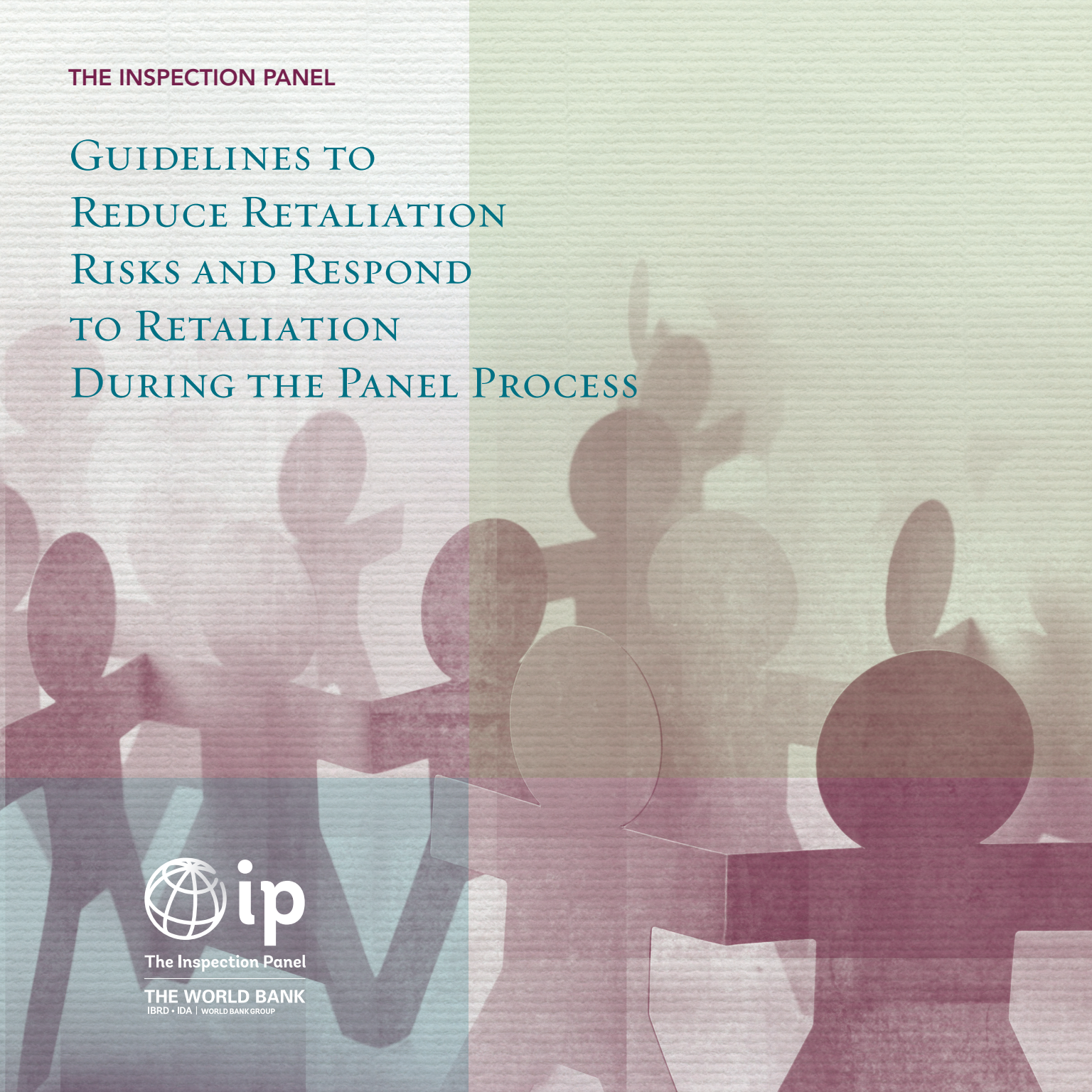
THE INSPECTION PANEL

Guidelines to Reduce Retaliation Risks and Respond to Retaliation During the Panel Process



The Inspection Panel

THE WORLD BANK

IBRD • IDA | WORLD BANK GROUP

INTRODUCTION

People who come to the Inspection Panel are often poor and/or vulnerable and lack voice or influence. They may fear that submitting a Request for Inspection to the Panel could be seen by some as a challenge, thus putting them at risk of retaliation. The Panel has experienced cases in which affected people have felt pressured during the Panel process. The Panel has stated that any form of retaliation threatens the integrity of the World Bank's accountability process, and may have long-term ramifications on a project's quality and the willingness of affected people to voice their concern about harm that might be caused by a Bank-financed project.

OBJECTIVES AND KEY PRINCIPLES

A fundamental premise of the Panel's function is that affected people can access it safely. With this in mind, the objective of these guidelines is to help reduce the risk of retaliation against Requesters, their Representatives and Associated Persons[1], and thus foster a safe environment for those seeking to work with the Panel.

These guidelines assist the Panel to (i) identify and monitor potential risks of retaliation, including emerging risks; (ii) plan and adopt preventive measures to address and reduce these risks; and (iii) identify appropriate responses if retaliation occurs.

The guidelines build upon the Panel's experience and established practice by other institutions, as well as informal consultations within the Bank, with accountability mechanisms of other organizations, and with relevant civil society organizations (CSOs).

1 STEP ONE: **RISK ASSESSMENT**

The risk of retaliation is assessed as soon as the Panel is approached, and it is reviewed throughout the Panel process. It is based on media reports, briefings by Country Office staff and the Bank's security personnel, and information provided by the Requesters and CSOs.

Risks are assessed in the context of their likelihood and severity, and are recorded in the Panel's internal "Key Issues Note" prepared for each case. The Panel reviews and updates these risk assessments at each stage of its process in consultation with Requesters and their Representatives, when risks emerge, or when an event increases the likelihood of retaliation. At all stages, the Panel prompts Requesters to think about their security issues and encourages them to report any threat or occurrence of retaliation.

In the event that the Panel's risk assessment deems the situation to be one where retaliation may materialize, the Panel will initiate discussions with Bank Management about steps that Management can take to enhance the security of the Requesters, their Representatives and Associated Persons.

2 STEP TWO: **IMPLEMENTATION OF PREVENTIVE MEASURES**

Preventive Measures. The Panel develops and adopts a plan—identifying preventive measures that are specific to each case and in accordance with the results of its risk assessment—in consultation with the Requesters and their Representatives and, when necessary, Bank Management and organizations that have specific expertise in protecting individuals at risk. Such measures will be sensitive to gender, race, ethnicity, age, disability, sexual orientation or gender identity, or other status. Measures can include suggestions for means and timing of communication, location and timing of meetings, means of transportation, use of trusted intermediaries, use and selection of interpreters, facilitators and other consultants, and use of specialized intermediaries for people with special needs. The Panel maintains the prerogative to implement the preventive measures it deems necessary.

If the Panel has a strong indication that, despite the adoption of preventive measures, interactions could lead to retaliation, it may temporarily decide not to contact Requesters, their Representatives or

Associated Persons, and will explain the reasoning behind its decision to relevant stakeholders.

Confidentiality. Requesters may ask for confidentiality in the handling of their Request. If Requesters wish that their names and personal information remain confidential, the Panel will keep such information strictly confidential from all involved in the process.[2] Confidentiality is a key principle of the Panel process. It covers the Requester's identity and information received from them in all forms (verbal, written and electronic) that may lead to their identity becoming known. Unless specific informed consent[3] is provided for the use of information, the Panel will not make use of it. When consent is granted, the Panel considers whether disclosure would result in retaliation and if so, the Panel will not disclose the information. When it is not clear that confidentiality is requested, the Panel attempts to confirm it. If that is not possible, the Panel assumes it is.

The Panel will clearly explain to the Requesters and their Representatives what it will do to maintain confidentiality, and any limitations on these efforts.

Site Visits. The Panel carefully plans the information-gathering process during its site visits, including the type of information needed, and how to access it. Regarding its site visits:

- The Panel relies primarily on the Requesters or their appointed representatives for planning.
- The Panel favors the choice of meeting locations suggested by Requesters. However, if the Panel deems the suggested location to be risky, it suggests alternative locations and/or proposes phone meetings or secure-correspondence exchanges.
- If documenting aspects of its work through photographs, the Panel will not utilize images of individuals at risk or indications of their location. The Panel seeks the consent of all individuals that may be identifiable in their photographs after providing information about how the photographs may be used.
- The Panel proposes follow-up meetings or conversations and suggests appropriate methods (phone calls, email, in person, etc.). The Panel maintains a log of such communications to record regular contacts and monitor security risks.

As required by its legal framework, the Panel keeps a low profile during its site visits to avoid media or other forms of public attention.[4]

Gathering and Protection of Information. During site visits, the Panel typically records information in notebooks or by using electronic devices but does not record the identity of Requesters or Associated Persons who have requested confidentiality. The Panel and its consultants keep notebooks and electronic devices in their personal care or in a secure place under lock. In areas where the security situation may be volatile, electronic information is kept in encrypted format and under password lock. The Panel and its consultants are expected to protect the information they carry and not share it.

Phone Calls and Verbal Communication. The Panel adopts a high level of care during phone conversations, even when there is no suspicion of eavesdropping. The Panel avoids discussions related to its work in public places or in the presence of others.

Interpreters and Facilitators. For meetings with communities, the Panel relies on interpreters or facilitators suggested by Requesters, as appropriate. The Panel must ensure that interpreters and facilitators understand the confidentiality requirements of their contracts as they relate to protecting the identities of those involved in the process from security threats. Since the Panel process may put interpreters and facilitators at risk, the Panel informs them of its risk assessment and gives them the opportunity to decline the assignment. The Panel keeps the personal and contact details of interpreters and facilitators confidential, and ensures that they hand over and delete all their notes in all forms (written, electronic, etc.) once their tasks are completed.

Transportation. The Panel carefully decides the choice of transportation. It may be advisable to

make use of taxis at random when needed or to use different vehicles throughout the course of the visit. Considering that the Panel's own security may be at stake, the final decision on whether to visit an area and how to reach it lies with the Panel in close coordination with the World Bank security services.

Monitoring. Throughout its process the Panel will actively monitor potential retaliation. That includes asking each of the complainants whether they or people closely associated with them had any security concerns or faced any problems, particularly following site visits. The Panel will provide all interviewees with the contact details for the Panel and urge them to contact the Panel, either directly or indirectly, should any security issue develop. The Panel will mention all instances of threats, intimidation or other retaliation in its eligibility and investigation reports, while respecting the confidentiality of complainants and interviewees, unless those affected request the Panel not to do so.

Cooperation with other IAMs. When the Panel cooperates with other Independent Accountability Mechanisms (IAMs) of International Financial Institutions during joint investigations, it must ensure that proper protocols are in place to guarantee the safety of information. Such IAMs must be duly informed of the Panel's risk assessment and these guidelines. Confidential information is not shared without the consent of the Requesters or Associated Persons.

3 STEP THREE: RESPONDING TO RETALIATION

If despite the adoption of preventive measures a threat materializes, the Panel gives immediate priority to such cases, corroborates the facts to the extent possible, implements the planned response developed with Requesters, and informs the appropriate levels of World Bank Management, including the President and the Board as necessary.

The Panel develops a protection timeline (with concrete escalatory steps) and considers the matter active until the safety of the person facing retaliation is guaranteed. The Panel does so in close coordination with the Bank's Senior Management, recognizing that in most cases it will be necessary for Bank Management to lead the efforts. Any proposed measures will prioritize the safety and well-being of those under threat.

GENERAL PROVISIONS

The Panel will ensure these guidelines are clearly posted on its website and that they are read together with the Operating Procedures and general guidelines for submitting a Request. In addition, they will be featured and widely disseminated in Panel outreach events.

The Panel's Executive Secretary will act as the overall focal point to coordinate its work preventing and responding to allegations of retaliation. Meanwhile, each assigned case officer will act as the focal point for the particular case at hand.

These guidelines will be reviewed against experiences in their implementation and amended as may be warranted.

ENDNOTES

1. "Associated Persons" are defined as those associated with the Panel process and may include project-affected persons, interviewees, and persons providing assistance to the Panel in the field (drivers, interpreters, facilitators, etc.).

2. The Inspection Panel at the World Bank. Operating Procedures. April 2014, paras. 14 and 18.

3. The person providing the consent needs to be properly informed about the precise meaning of confidentiality, the manner in which the information may be used by the Panel, how the information will be protected, and implications of the use of information for their safety and well-being. Special efforts must be made to ensure that children and their guardians understand confidentiality and the need for it.

4. 1999 Clarification of the Board's Second Review of the Inspection Panel, paragraph 12.

The Inspection Panel | World Bank | 1818 H Street, NW | Washington, DC 20433 | @InspectionPanel
Telephone: (202) 458-5200 | Fax: (202) 522-0916 | Email: ipanel@worldbank.org | Website: www.inspectionpanel.org