

---

## Appendix 2 Summary feedback on CORE’s draft retaliation framework

---

### Background

The CORE shared 5 draft documents with the CNCA that outline its proposed retaliation framework. These include:

- “What is retaliation,” a short document that defines retaliation, states that the CORE takes it seriously, highlights the risks and key agents to consider with respect to retaliation.
- “CORE’s approach to retaliation,” a short document that outlines the CORE’s approach to retaliation: described as assess, reduce, respond, report.
- “Information for Individuals and Communities” includes commitments by the CORE to keep information confidential; suggestions on how communities can reduce risk of retaliation (with advice that human rights defenders should not: “say or do things that might make others angry with you... take action against others who you think are retaliating against you or may do so, even if you think they are guilty”).
- “Information for Companies” explains risks to companies for failing to take retaliation seriously and makes suggestions to companies (i.e. zero tolerance policies...).
- “Retaliation Risk Assessment Tool”.

### Importance of an effective retaliation and reprisal framework

Human rights defenders around the world, particularly those working on business and human rights issues, face serious risks because of the nature of their work. When individuals and communities seek to access remedy for harms, they often face reprisals and retaliation.

**Given that the CORE does not have any independent investigatory powers to distinguish it from the National Contact Point, we would recommend that it closely examine the well-documented critiques of Canada’s National Contact Point, particularly with respect to risks of harm and retaliation.<sup>1</sup>**

For example, the Business and Human Rights Resource Centre and OECD Watch report that:

Among 250 specific instances filed by NGOs or communities since 2006, **at least 25% involved reprisals** against complainants or others working on the same situations of harmful business activity. This number is likely a very low estimate, as most reprisals are unreported. For defenders and affiliates, filing an NCP case may deepen risk of reprisal by raising

---

<sup>1</sup> OECD Watch’s recommendations to the NCP on retaliation are included as an addendum.

company and host-government awareness of defenders' identities and activities.

According to the same report, the industries within the CORE's purview (mining, oil and gas, garment) account for 57% of all reprisals.<sup>2</sup>

Development of a draft retaliation framework is an important step to acknowledge the seriousness of the issue and demonstrate concern for impacted communities. The CORE's draft framework includes some important elements, such as:

- a clear statement that the CORE takes retaliation seriously
- recommending a zero tolerance policy on retaliation throughout companies' global operations
- expressing a commitment to support impacted communities, including to:
  - “think about how (CORE's) work may increase the risk of retaliation. We do this before we engage and throughout our engagement ...We will try to find safer ways to stay in contact, travel, get information and protect witnesses, interpreters and others,”
  - keep information confidential,
  - talk with complainants about the risks to make sure the CORE has informed consent before taking any steps and to talk to complainants about ways to respond,
  - not take any steps without complainants' consent,
  - try to stay in regular contact with complainants or, if it is not safe for complainants to communicate with the CORE, with people or organizations that represent complainants' interests, and to
  - monitor retaliation
- being transparent about (some of) the limitations of the CORE
  - stating that CORE does not have the legal power to protect individuals and communities from retaliation<sup>3</sup>

---

<sup>2</sup> <https://www.oecdwatch.org/wp-content/uploads/sites/8/2019/06/Reprisals-NCP-system.pdf>

<sup>3</sup> The Green Climate Fund's Independent Redress Mechanism (IRM)'s Supporting Operating Procedures on Retaliation go further: <https://irm.greenclimate.fund/documents/1061332/1197271/SoP+Module+8+-+Retaliation.pdf/4b2d9377-ea2b-4021-6294-6df44fe3f258>

“Recognising limits 15. While the IRM is committed to minimising the risks of retaliation in relation to its processes, it also recognises the limitations it faces in its ability to mitigate risks and protect those involved. The IRM does not have a continuing presence at GCF project or programme locations nor established channels of communication with all those who may, where appropriate, be invited to use their good offices to minimise risks of retaliation. The IRM has no direct power to physically protect persons involved in IRM processes and does not purport to replace national or international judicial bodies, or law enforcement agencies whose functions include protecting the public in such situations. In addition, the GCF and its staff do not have privileges and immunities in all countries in which it operates and therefore may lack legal protection if they were to become involved in protecting complainants or requesters from retaliation, particularly from governments themselves.

However, despite these positive elements, the policy is not sufficiently robust.

Informed decision-making requires transparency about CORE’s lack of powers

As indicated in the retaliation documents itself, “CORE does not have the legal power to protect individuals and communities from retaliation.” **It should also be made explicit that the CORE does not have the legal authority to require companies to provide the information that it needs in order to investigate community allegations about business-related harms.**

**The CORE has expressed a commitment to enable communities to make informed decisions about retaliation. This requires that the office be transparent with impacted communities and workers, and those who support them, that the CORE as structured is a voluntary dispute resolution mechanism that relies on the good will of companies to operate.** It would be highly irresponsible for the CORE to open its doors to complaints, putting communities and individuals at risk of reprisal, without being explicit about the office’s serious limitations. This includes making public the CORE’s own conclusion that it needs the power to compel documents and testimony in order to be effective.

The retaliation report section of the framework states that the “CORE can also provide remedies for retaliation.” This is not explained. Greater clarity is required for potential complainants to weigh potential benefits and consequences of bringing a complaint. **The framework must be explicit that any recommendations for remedy made by the CORE are non-binding on all actors.**

CORE site-visits and community engagement protocols

The CNCA raised serious concerns with the CORE in February 2020 regarding an international trip that the office was planning. That trip included a visit to a controversial project site in Colombia, in response to a request from the company involved, and without prior consultation with impacted communities or civil society. Nor was there any indication that the CORE had assessed the risks posed to local communities from making such a trip. The CORE informed the CNCA that it was developing protocols that it would use to guide its decision-making regarding future requests for site visits. The CNCA has not been informed about the content of any such protocols. **The retaliation framework shared here does not replace site visit protocols, and should be expanded to specifically address this point.**

### Lack of clarity on how confidentiality will be maintained and from whom

- We support the CORE's commitments to ensure the confidentiality of vulnerable persons (where they request it) and to permit anonymous complaints.
- It is not clear that any CORE staff have experience working directly with impacted communities outside of Canada or in investigating international human rights harms - particularly those linked to large multinational corporations operating in remote areas of the world. This is likely to impact the CORE's ability to properly serve these communities or to effectively work with them to institute adequate retaliation-avoidance and response measures.
- Furthermore, this lack of experience may prevent the CORE from correctly identifying what information could lead to the identification of complainants or individuals for whom the CORE has endeavored to maintain confidentiality. This concern is heightened because of the CORE's plans to share information with, and rely on guidance developed by, other government departments - including those that are responsible for promoting Canadian business interests overseas (i.e. Global Affairs Canada, National Contact Point, embassies).
- Because the CORE was created via OIC under the Public Service Employees Act, rather than the Inquiries Act or novel legislation, and because no consequential amendments to the Access to Information Act have been made, the CORE may be unable to adequately protect the confidentiality of documents it receives from impacted communities. This should be made explicit to the public.

### CORE asserts that its approach is based on best-practices

The CORE's approach to retaliation is described as being based on "best practices, research and established guidance." The CORE shares a lengthy list of resource materials and tools that it studied in the development of its retaliation strategy. However, the CORE does not make clear how these frameworks, which are much more comprehensive than CORE's approach, informed its strategy. In fact, its strategy appears to be at odds with leading frameworks in the field. For example, CORE advises individual complainants not to "say or do things that might make others angry with you" or to "take action against others who you think are retaliating against you or may do so." Other organizations, with deep expertise and lengthy experience accompanying individuals and communities at risk, do not issue such advice.

**The CORE should amend its framework to ensure consistency with good practice.** Given the office's lack of expertise and experience accompanying individuals and communities at risk, it is preferable that the **CORE refer potential complainants to the security and safety protocols developed by leading organizations in the field**, rather than issuing such advice itself.

### CORE and independence from government?

The retaliation framework highlights numerous instances where CORE will work with Canadian government departments (i.e. “We work with Global Affairs Canada to develop and apply the best responses”; and references to the National Contact Point) or will rely on government guidelines (i.e. in detailing best practices). However, it does not mention how CORE will ensure that confidential information will be kept from these entities.

We encourage the CORE to continue to take seriously the risks faced by human rights defenders, women, Indigenous peoples and workers around the globe. In particular, we recommend the following:

1. Given that it is impossible to eliminate all risk of reprisal or retaliation, CORE should advocate more forcefully for the Government of Canada to provide it with the basic minimum powers needed to be effective so that communities and individuals putting themselves at risk by making a complaint have some prospect that the CORE process will help them access remedy and hold companies to account.
2. The CORE should create a more comprehensive retaliation framework, building on the feedback provided above and - where appropriate - incorporating best practice directly and fully.

**Addendum: OECD Watch and Business and Human Rights Resource Centre**  
**Suggested Actions for States and NCPs regarding reprisals, available here:**

<https://www.oecdwatch.org/wp-content/uploads/sites/8/2019/06/Reprisals-NCP-system.pdf>

- Publicly and broadly condemn reprisals against defenders.
- Ensure all NCP staff know the risks in sectors and regions and appoint designated staff prepared and equipped to respond to potential and actual attacks.
- Publish general guidelines to prevent and respond to potential or actual reprisals against defenders. Every case will require a unique response, such as more or less confidentiality, fast-tracking or delaying of the case, special mediation steps, etc.
- Raise awareness among MNEs about how businesses are involved in perpetrating and condoning harms to defenders.
- Ensure complainants have many secure ways to file complaints (web, mail, text, phone) and know how to use them.
- Proactively protect confidentiality of complainants' identities, unless and until visibility will help protect complainants.
- Proactively ask complainants about threats in every case.
- Consult complainants and defender experts as soon as risks are identified by a party or NCP; monitor threats during the case.
- Ensure mediation terms include a no reprisals clause.
- Improve intra- and inter-government coordination to enable speedy and appropriate response to reprisals.
- Follow-up after complaint process to check defenders' safety.
- Help businesses know how to prevent and respond to threats by their staff, subsidiaries and partners, and host governments.
- Make human rights due diligence mandatory to ensure companies identify and respond to risks to defenders.
- Sanction companies repeatedly linked to harms to defenders.