COMMONWEALTH OMBUDSMAN

ASSESSING AND MANAGING THE RISK OF REPRISAL

1. Introduction:

For the Public Interest Disclosure (PID) Scheme to function as intended under the *Public Interest Disclosure Act 2013* (the PID Act), disclosers must be able to make disclosures without the fear of retaliation from individuals or agencies. Your Agency has a responsibility to ensure that parties who make disclosures relating to your Agency are protected from reprisal. Your Agency is legally required to have procedures in place to assess and mitigate the risk of reprisal.[1] This document will assist your Agency in designing and implementing such procedures.

1.1 Why is a risk of reprisal plan important?

A robust and well-publicised risk of reprisal assessment plan is an important part of encouraging an organisation's pro-disclosure culture. Almost a quarter of people who had witnessed but not reported wrongdoing claim that fear of reprisal had prevented them from doing so.[2] The existence of a risk of reprisal plan can help to assuage this fear, particularly where, as discussed below, the plan is well-known to staff members and forms a part of the Agency's culture. This in turn leads to more potential disclosers coming forward, allowing agencies to deal with problems internally before they escalate.

1.2 What is reprisal?

Reprisal is broadly defined in the PID Act. Section 13 of the PID Act defines a reprisal as any act or omission which causes detriment to a person where that act or omission is a result of someone else's belief that the person made a PID.

The Office of the Commonwealth Ombudsman (the OCO) has in the past encountered cases where reprisal has taken the form of:

- bullying and harassment of disclosers;
- negative professional consequences such as being passed over for promotion or not having contracts for services renewed; and
- threats of physical violence.

It is important to note that reasonable administrative action taken to protect a person from detriment, such as moving them or someone else to a different work area, is not reprisal.[3]

---

[1] *Public Interest Disclosure Act 2013,* s59(1).
[2] AJ Brown (ed) *Whistleblowing in the Australian Public Sector: Enchancing the Theory and Practice of Internal Witnesss Management in Public Sector Organisations* (2008) ANU E Press, 72.
[3] *Public Interest Disclosure Act 2013,* s13(3).

Additionally, disciplinary action taken against disclosers or suspected disclosers will not be reprisal unless it is motivated by the fact that someone has or is suspected of having made a PID.

It is possible for a third party to take reprisal action against a discloser. For example, a manager may move someone they perceive as a "troublemaker" out of their team. The fact that someone other than the subject of the disclosure is taking the action does not prevent the action from being a reprisal.

2. Legal obligations:

The Principal Officer of an Agency, typically the Agency Head or a person listed by the PID Act as the Principal Officer, is required to establish procedures for handling PIDs within their Agency.[4] Such procedures must include mechanisms for assessing the risk of reprisal against parties who make PIDs about their Agency.[5] Note that, by contrast, PID handling procedures are not specified within the legislation.

The Principal Officer of an Agency also has a responsibility to protect public officials within their Agency from reprisals.[6] The legislation is not overly prescriptive, but the OCO suggests that without a plan to identify and mitigate the risk of reprisal, it will not be possible for Principal Officers to fulfil this obligation.

There are a number of other sections in the PID Act which, while not relating directly to an Agency's reprisal obligations, need to be considered when drafting a reprisal risk plan:

- Reprisal action, or threatening to take reprisal action, against someone who has made a PID or whom a party suspects of making a PID is a criminal offence punishable by up to two years imprisonment;[7]
- Where a reprisal occurs or is threatened, it is possible for the discloser to take various forms of legal action to prevent or mitigate the reprisal;[8]
- Confidentiality provisions apply to information obtained during the course of a PID investigation or information about the identity of a discloser; and[9]
- The fact that much of the PID Act (for example, ss 43 to 45) is directed towards the manner in which agencies must process and allocate PIDs.

All of these factors need to be taken into account when creating a risk assessment procedure.

2.1 Policy obligations:

---

[4] *Public Interest Disclosure Act 2013* s59(1).
[5] Ibid s59(1)(a).
[6] Ibid s59(3)(a)
[7] Ibid s19
[8] Ibid ss14, 15, 16.
[9] Ibid ss20, 65.

There are whole-of-government policy obligations which apply in the risk management space. These policy obligations are derived primarily from s 16 of the *Public Governance Performance and Accountability Act 2013* (the PGPA Act). The PGPA Act requires Commonwealth entities to establish and maintain a system of risk oversight and management. The Department of Finance has created policy guidelines for Commonwealth entities to meet this requirement. These guidelines are available at http://www.finance.gov.au/sites/default/files/commonwealth-risk-management-policy.pdf. The guidelines explain what is expected from risk plans more generally and can be usefully adapted to risk of reprisal plans.

Importantly, these guidelines prevent this office from producing a generic risk assessment plan. While we are able to provide guidance on how risk of reprisal plans can be drafted, ultimately the responsibility for drafting such a plan rests with the Agency to which it applies.

The guidelines require all agencies to generate risk assessment plans which are endorsed at a high level. Research suggests that having senior leadership demonstrate positive and accountable behaviour increases the likelihood of disclosures.[10] The guidelines outline the Commonwealth's expectations about the features of such a plan, many of which can also be applied to lower-level risk of reprisal plans. The guidelines also refer to creating a positive culture around handling risk. Organisational culture is a big part of these guidelines, which mirrors its importance in the PID space.

2.1.1 Who is responsible for managing reprisal obligations?

As discussed, the Principal Officer of an Agency is legally responsible for ensuring that an Agency has an adequate risk of reprisal plan. In practice, we suggest that the plan be drafted primarily by staff responsible for your Agency's integrity procedures, as they are likely to be most familiar with the risks involved in conducting investigations. We suggest that your agency's human resources (HR) and Legal areas have input into the plan. Your HR area will need to manage the relationships between the staff members involved and be aware that there may be a period of tension in the workplace, as well as enacting the practical aspects of any risk management plan such as organising staff leave or enabling secondments to different areas. Your Legal area will need to ensure that the plan complies with the Agency's legal obligations and controls both for the risk of reprisal through the courts and for the legal action a party who has been the victim of reprisal can take.

3. Our expectations:

As the Agency responsible for the PID Scheme, the OCO has certain expectations as to what features a risk assessment will have. While these expectations are not binding, we advise that any risk assessment plan containing these features is more likely to meet your Agency's legal obligation to provide a plan which protects staff from the risk of reprisal.

---

[10] James Gerald Callier, "Transformational Leadership and Whistle-Blowing Attitudes: Is this Relationship Mediated by Organizational Commitment and Public Service Motivation?" 45(4) *American Review of Public Administration* 2013, 458.

3.1: Timeliness: Our expectation is that risk assessments are conducted as soon as possible after the PID is received. This distinguishes a risk of reprisal plan and an Agency-wide risk assessment plan; wheras Agency-wide plans usually deal with risks on a grand scale, thereby requiring longer to assess and respond to them, a reprisal plan is more self-contained.

It is also worth noting that, while the PID Act contains timelines for allocation and investigation of PIDs, there are no required timeframes relating to the content of PIDs. It is therefore possible for a discloser to make a PID about a situation that has been ongoing for some time, in which they are involved and in which they are at risk of reprisal. This makes it important that plans and responses commence as soon as possible. Additionally, a risk plan which forces agencies to respond quickly and concretely to disclosures has the benefit of being seen to be working, which in turn increases a discloser's confidence in the plan.

3.2: Subject matter: Our expectation is that an Agency plan would contain a list of potential risks against which the individual discloser's situation could be addressed. This is similar to the way Agency-level risk plans work, in that they will usually have a set list of risks which need to be taken into account.

The OCO has produced a list of common risk factors which can be found at **Table One**. We expect that a risk of reprisal plan will cover all of these factors at a minimum, as well as any organisation-specific risks that you become aware of in the course of your work.

Of particular importance is the relationship between the discloser and the subject of the disclosure. We expect that any risk assessment plan will examine, at a minimum:

- whether the discloser and the subject work together;
- whether they are in each other's reporting lines or have managers or staff in common;
- whether they are physically located in the same office; and
- whether they socialise outside of work.

These are all potential risk factors which need to be addressed.

3.3: Solutions: Our expectation is that as well as identifying risk factors and likely outcomes if those factors are not addressed, risk of reprisal plans will also contain strategies to mitigate the risks of reprisal. In the past, this Office has seen strategies such as separating the officers in question, finding alternate work for one or both parties and making sure the subject of the disclosure is aware of the serious criminal penalties for taking reprisal action. Any solution must be compatible with the confidentiality requirements in ss 20 and 65 of the PID Act, noting that these confidentiality requirements will not usually provide any impediment to actions taken to assist the discloser or the subject of the disclosure.

As well as providing concrete plans of action, the existence of these strategies can prove invaluable when defending an Agency against allegations of reprisal. The OCO has seen cases where a discloser has had to be moved to protect them from reprisal. If a discloser were to subsequently allege that their move had been reprisal, the Agency would be able to show that the move was in fact motivated by the risk of reprisal identified by the plan.

We note also that some agencies provide assistance to the discloser and/or the person who is the subject of a disclosure, for example in the form of counselling or access to a support person during the process. Where this assistance exists, it should be represented in the risk of reprisal plan.

3.4: Change over time: Our expectation is that risk of reprisal assessments are living documents – that is, they are constantly referred to and updated as circumstances change. A demonstration of this interaction is set out at **Table Two**. We expect that risk assessment plans will be generated as soon as the disclosure is made and reviewed upon commencement of any investigation and the finalisation of any investigation. Additionally, the circumstances of the case may change in such a manner that a new risk assessment is required. In particular, it is possible for PID investigations to be closed down so that the same conduct can be investigated under Code of Conduct or Fraud procedures. These separate procedures may have their own risk mitigation mechanisms or bring with them additional risks, so it is important that the risk of reprisal plan be updated to reflect them.

In our experience, the best risk assessment procedures involve constant communication with the discloser to determine whether the plan needs to be updated. As well as making the document responsive, our experience has been that involving disclosers as closely as possible increases their positive experience of the PID process. Organisation-wide confidence in the process leads, in turn, to the PID Scheme being utilised more frequently.

3.5: Access and recording: Our expectation is that the plans described above will be written down and will be accessible to the relevant stakeholders according to your Agency's standard records management procedures. This is to ensure that the situation will continue to be monitored and mitigation strategies will continue to be implemented. It also has the advantage of making those plans easily accessible to disclosers, as well as to this office in the event that a complaint is made about your Agency's handling of a PID. Accessibility of such documents can lead to increased confidence in the process for current or potential disclosers.

It is important to note that confidentiality restrictions in the PID Act are likely to apply to this information. Section 20 of the PID Act makes it an offence to disclose the identity of a person who has made a PID outside of certain circumstances. This is most relevant where the disclosure is made for the purposes of the PID Act or another law of the Commonwealth or a State or Territory.[11]

Similarly, s 65 of the PID Act restricts the use or disclosure of information obtained during the course of conducting a PID investigation.[12] It also restricts how information obtained in connection with the

[11] *Public Interest Disclosure Act 2013*, ss20(3)(a), 20(3)(d).
[12] Ibid ss65(1), 65(2).

exercise of a power or performance of a function under the PID Act is used or disclosed. While these provisions are unlikely to affect how a reprisal plan is used for the purposes of preventing reprisal, access to such a plan does need to be controlled so that the provisions are not accidentally breached.

4. Enforcement difficulties:

It is important to understand that these plans are oriented around preventing reprisal from taking place, rather than responding to it once it has occured. This is quite intentional - since it is difficult to prove that reprisal action has taken place. While the PID Act does empower disclosers to take legal action to prevent or remedy reprisals which have been taken against them, the onus is on the discloser to take that legal action, meaning that it may not be available as a solution in all cases.[13] Similarly, prosecution for the criminal offence of reprisal has never been attempted at the Federal level, and cases where similar offences at the state level have failed, demonstrating the difficulties of proving that an action was reprisal as opposed to simply being part of the ordinary process of office management.

As well as being difficult for disclosers to enforce their rights, legal action of this type carries significant risks for organisations. As well as the cost and difficulty associated with legal action, there are reputational risks to being involved in matters of this type. This is particularly important in the PID space given that, as discussed above, having to go to court to enforce one's PID Act rights is likely to be seen by potential disclosers as a deterrent and thus make them less likely to disclose. It is therefore far better to prevent reprisals from occurring or to stop them from escalating to a point where legal action is necessary.

[13] Ibid ss14, 15, 16.

TABLE ONE: INDICATORS OF A HIGHER RISK OF REPRISAL OR WORKPLACE CONFLICT[14]

Threats or past experience	Has a specific threat against the discloser been made? Is there a history of conflict between the discloser, management, supervisors or colleagues? Is there a history of reprisals or other conflict in the workplace? Is it likely that the disclosure will exacerbate this?
Confidentiality unlikely to be maintained	Who knows that the disclosure has been made or was going to be made? Has the discloser already raised the substance of the disclosure or revealed their identity in the workplace? Who in the workplace knows the discloser's identity? Is the discloser's immediate work unit small? Are their circumstances, such as the discloser's stress level, that will make it difficult for them not to discuss the matter with people in their workplace? Will the discloser become identified or suspected when the existence or substance of the disclosure is made known or investigated? Can the disclosure be investigated while maintaining confidentiality?
Significant reported wrongdoing	Are there allegations about individuals in the disclosure? Who are their close professional and social associates within the workplace? Is there more than one wrongdoer involved in the matter? Is the reported wrongdoing serious? Is or was the reported wrongdoing occurring frequently?

[14] Adapted from NSW Ombudsman, *Managing risk of reprisals and conflict*, Public Interest Disclosure Guideline C4, p. 3.

	Is the disclosure particularly sensitive or embarrassing for any subjects of the disclosure, senior management, the Agency or the government? Do these people have the motivation to take reprisals – for example, because they have a lot to lose? Do these people have the opportunity to take reprisals – for example, because they have power over the discloser?
Vulnerable discloser	Is or was the reported wrongdoing directed at the discloser? Are there multiple subjects of the disclosure? Is the disclosure about a more senior official? Is the discloser employed part-time or on a casual basis? Is the discloser isolated – for example, geographically or because of shift work? Are the allegations unlikely to be substantiated – for example, because there is a lack of evidence? Is the disclosure being investigated outside your organisation?

TABLE TWO: CREATING AND UPDATING A RISK OF REPRISAL PLAN