Australian Government

National Indigenous Australians Agency

Public Interest Disclosure Procedures

I, Rachael Jackson, Chief Operating Officer and delegate of the Principal Officer of the National Indigenous Australians Agency, revoke all previous versions of the Public Interest Disclosure Procedures of the National Indigenous Australians Agency and establish the following procedures under subsection 59(1) of the *Public Interest Disclosure Act 2013* (Cth).

These procedures commence upon signature.

Rachael Jackson

Chief Operating Officer

17 November 2020

Public Interest Disclosure Procedures

1. Overview

Purpose

1.1 The purpose of these procedures is to provide advice and guidance to National Indigenous Australians Agency (NIAA) employees about the management of public interest disclosures (PIDs) made by a discloser under the *Public Interest Disclosure Act 2013* (Cth) (PID Act). These procedures apply to allegations of disclosable conduct and sets out the following information:

- What is a public interest disclosure?
- Who can make a public interest disclosure?
- How to make a public interest disclosure
- The NIAA's management of public interest disclosures and how they are investigated

Authority

1.2 Section 59 of the PID Act.

Statement of Commitment

1.3 The NIAA is committed to the highest standards of ethical and accountable conduct, and will ensure that those who report, or who are considering making a report about disclosable conduct, are supported and protected from any adverse consequence relating to the disclosure in accordance with the PID Act.

1.4 The NIAA will ensure that any disclosures made under the PID Act are managed in accordance with the PID Act and dealt with confidentially. In order to uphold the good reputation of the NIAA and to provide a safe and ethical workplace, public officials who are aware of suspected wrongdoing in the NIAA (or elsewhere in the Commonwealth public sector) are encouraged to report such instances in accordance with the provisions set out in these procedures.

Definitions

1.5 The full definitions of the following terms are set out in the PID Act. The definitions apply for the purposes of these procedures. In summary, key definitions are:

1.6 ***Authorised Officer*** means the Chief Executive Officer (CEO), or an agency officer appointed in writing by the Principal Officer (or delegate) as an authorised officer for the purposes of the PID Act. Authorised Officers receive public interest disclosures, provide advice to disclosers about the PID Act and allocate disclosures, when necessary.

1.7 ***Disclosable Conduct*** is conduct (including omitting to do an act) by an agency or by a public official in connection with his or her position as a public official that:

- contravenes a law of the Commonwealth, a State or a Territory;
- occurs in a foreign country and contravenes a law in force in that country that applies to the agency or public official and that corresponds to a law in force in the Australian Capital Territory;
- perverts, or attempts to pervert, the course of justice or involves corruption of any other kind;

- constitutes maladministration, including conduct that:
  - is based on improper motives:
  - is unreasonable, unjust or oppressive: or
  - is negligent;
- is an abuse of public trust;
- is fabrication, falsification, or deception in relation to scientific research, or misconduct in relation to scientific work;
- results in the wastage of public money or public property, or of the money or property of an authority covered by the PID Act;
- unreasonably results in a danger to the health and safety of a person or persons, or unreasonably results in or increases the risk of a danger to the health and safety of a person or persons;
- results in a danger to the environment, or results in or increases the risk of a danger to the environment;
- is prescribed by the PID Rules under section 83 of the PID Act; or
- is engaged in by a public official that:
  - involves abuse of the public official's position; or
  - could, if proved, give reasonable grounds for disciplinary action against the public official.

1.8 It does not matter when the disclosable conduct occurred.

1.9 It does not matter whether the public official who carried out the alleged conduct has ceased to be a public official since the time the conduct is alleged to have occurred, but it is necessary that they carried out the conduct in connection with their position as a public official.

1.10 ***Discloser*** means an individual who discloses information.

1.11 ***Disclosure*** means information disclosed by a discloser.

1.12 ***Investigating Officer*** means a delegate of the Principal Officer who has the power to investigate a disclosure.

1.13 ***PID Act*** means the *Public Interest Disclosure Act 2013* (Cth).

1.14 ***Principal Officer*** means the CEO of the NIAA or their delegate/s as appointed from time to time.

1.15 ***Public Official*** is defined under the PID Act and includes:

a) a Commonwealth public servant;
b) Member of the Defence Force;
c) Appointee of the Australian Federal Police;
d) Parliamentary Service employees;
e) Director or staff member of a Commonwealth company;
f) Statutory office holder or other person who exercises powers under a Commonwealth law; or
g) Individuals and organisations that provide goods or services under a Commonwealth contract, including subcontractors who are responsible for providing goods or services for a Commonwealth contract.

1.16 ***Public interest disclosure*** means a disclosure made by a discloser who is or has been a public official to an Authorised Officer or a supervisor of the discloser with information that the discloser believes on reasonable grounds tends to show, one or more instances of disclosable conduct.

2. Making Disclosures

Who can make a public interest disclosure?

2.1 A current or former public official can make a public interest disclosure under the PID Act. They can do so anonymously or openly. They do not have to state or intend that they are making the disclosure for the purposes of, or under the PID Act.

What can be reported?

2.2 A current or former public official can disclose information that they believe on reasonable grounds tends to show disclosable conduct.

How can a public interest disclosure be made?

2.3 A current or former public official can make the disclosure in person, by telephone or in writing, including by email, and can remain anonymous to an Authorised Officer or their supervisor. The NIAA encourages disclosers to submit their disclosure by contacting an Authorised Officer, as they are trained to receive disclosures and provide information on the process to make a disclosure and the protections given to disclosers under the PID Act. If a disclosure is made to the discloser's supervisor, then the supervisor must refer the disclosure to an Authorised Officer as soon as reasonably practicable.

2.4 Disclosures can be made anonymously. Disclosures are considered anonymous if:
a) the identity of the discloser is not revealed and if no contact details for the discloser are provided; or
b) the discloser does not disclose their name but does provide anonymous contact details.

2.5 Disclosures that are made anonymously may prevent an Authorised Officer from assessing or otherwise managing the disclosure. Furthermore, it may prevent the Principal Officer or their delegate/s to properly investigate the disclosure.

2.6 A list of the current NIAA Authorised Officer can be found on the Intranet and on the external website.

What is not disclosable conduct?

2.7 Individual grievances or workplace conflicts would generally be dealt with by other existing NIAA processes rather than as the subject of investigation under the PID Act. Matters that reflect private or personal interest are generally not matters of public interest. This includes:
- Personal disagreement with a government policy or proposed policy;
- Personal disagreement with an action or proposed action by a minister, the Speaker of the House of Representatives or the President of the Senate; and
- Expenditure or proposed expenditure related to such policy or action.

2.8 If an NIAA employee has a complaint that does not fall within the definition of disclosable conduct but nevertheless wishes to raise the issue with management, or if the employee wishes to raise a matter informally, depending on the nature of the issue, the employee is encouraged to approach their supervisor to obtain advice in the first instance.

Protection for disclosers

2.9 A discloser is protected from reprisal action under the PID Act unless such a disclosure does not fall within the Act. Those protections include confidentiality and immunity from criminal and civil liability or disciplinary action. The PID Act does not place any time limits on protections.

2.10 However, making a disclosure under the PID Act does not protect a discloser from their own wrongdoing. A discloser who intentionally makes a false or misleading disclosure will not receive protections under the PID Act.

2.11 When a disclosure is made and determined to be a disclosure under the PID Act, an Authorised Officer or supervisor will conduct a risk assessment, within 14 days after the disclosure is received, that considers the risk of reprisal action taken against the discloser. The NIAA will provide support to disclosers, regardless of the result of that risk assessment, and where necessary will develop a risk mitigation strategy.

3. Roles and Responsibilities

Authorised Officers

3.1 Authorised Officers have a range of decision-making, notification and other responsibilities under the PID Act, including:

- receiving disclosures from current or former public officials who belong to the NIAA;
- receiving disclosures from other public officials about conduct concerning their agency;
- deeming a person to be a public official to allow them to make a public interest disclosure;
- explaining the requirements of the PID Act to disclosers;
- advising disclosers of any designated publication restrictions that apply to the information they have disclosed;
- assessing disclosures to determine whether the information provided could be considered to be a public interest disclosure;
- making any preliminary inquiries necessary to make an allocation decision;
- using their best endeavours to allocate all or part of the disclosure to the Principal Officer of the NIAA for handling and/or another Commonwealth agency that has agreed to handle the disclosure, within 14 days after the disclosure is made to the Authorised Officer;
- notifying the Principal Officer or their delegate/s of NIAA of the allocation decision, the details of the disclosure and, if the discloser consents, the discloser's identity;
- if any other Commonwealth agency has agreed to handle the disclosure, notifying the Principal Officer of that Commonwealth agency of the allocation decision, the details of the disclosure and, if the discloser consents, the discloser's identity;
- notifying the Ombudsman (or Inspector General of Intelligence and Security (IGIS) where appropriate) of the allocation decision, the details of the disclosure and, if the discloser consents, the discloser's identity;
- informing the discloser of the allocation decision, where practicable, within 14 days;
- consenting to the allocation of a disclosure by an Authorised Officer of another Commonwealth agency; and

- advising the discloser of a decision not to allocate, where practicable within 14 days, the reasons why and any other course of action that may be available under Commonwealth law.

Principal Officer

3.2 Under the PID Act the Principal Officer of the NIAA is the CEO. There are a number of responsibilities for the Principal Officer, including establishing procedures for managing public interest disclosures, investigating and providing reports on disclosures, undertaking risk assessments and ensuring that appropriate action is taken in relation to recommendations arising from an investigation.

3.3 The CEO has delegated all of his powers and functions under the PID Act.

Public Officials and All Staff

3.4 The PID Act requires all public officials to use their best endeavours to assist the Principal Officer or their delegate/s in the conduct of an investigation. They must also use their best endeavours to assist the Commonwealth Ombudsman in their functions under the PID Act. Beyond those specific responsibilities, all NIAA employees share the responsibility of ensuring the PID Act works effectively. Their role includes:
- reporting matters where there is evidence that shows or tends to show disclosable conduct;
- identifying areas where there may be opportunities for wrongdoing to occur because of inadequate systems or procedures, and proactively raising those with management;
- supporting staff known to have made public interest disclosures; and
- keeping confidential the identity of a discloser and anyone against whom an allegation has been made, if they become aware of those matters.

Supervisors

3.5 Under the PID Act, a supervisor is a public official who supervises or manages the person making the disclosure.

3.6 If the supervisor has reasonable grounds to believe that the information given to them concerns, or could concern, disclosable conduct, they must give that information to an Authorised Officer as soon as reasonably practicable. However, because of the confidentiality requirements, the supervisor should obtain the discloser's consent before passing on the discloser's identifying particulars to an Authorised Officer.

3.7 Supervisors also have a key role in ensuring that the NIAA's workplace culture supports the making of public interest disclosures in a safe environment. They can help to do so by:
- being knowledgeable about the PID Act and these procedures, particularly in relation to confidentiality requirements;
- being approachable to staff who wish to report serious misconduct;
- ensuring staff undergo available training;
- confronting any workplace prejudices about making a disclosure;
- supporting a staff member who they know has made a public interest disclosure and ensuring they are protected from reprisal action;
- increasing management supervision of the workplace if necessary (for example, if workplace conflict occurs because a disclosure has been made or an investigation is under way);
- ensuring identified problems in the workplace are corrected; and

- leading by example for their staff.

Legal Services Branch

3.8 Legal Services Branch are responsible for notifying the CEO via the Chief Operating Officer upon receiving a new disclosure under the PID Act.

3.9 Legal Services Branch are responsible for notifying the CEO via the Chief Operating Officer if an Authorised Officer allocates a disclosure to NIAA in accordance with paragraph 5.8.

4. Procedures for Supervisors

4.1 A supervisor has specific obligations under the PID Act to refer a disclosure to an Authorised Officer where:
   a) a staff member they manage or supervise discloses information to them; and
   b) the supervisor has reasonable grounds to believe that the information concerns or could concern disclosable conduct.

4.2 Before referring a disclosure to an Authorised Officer, the supervisor must, as soon as reasonably practicable:
   a) make a written record of the facts of the disclosure, including the time and date of the disclosure;
   b) if the discloser wishes to remain anonymous, conduct an assessment of any risk that reprisal action might be taken against the discloser (see Appendix 1-Risk Assessment Information);
   c) seek consent from the discloser to include the discloser's name and contact details in the written record; and
   d) ask the discloser to sign the record of disclosure, where this is practicable.

4.3 At the time a supervisor gives information to an Authorised Officer, the supervisor must also, as soon as reasonably practicable:
   a) give the Authorised Officer all records in relation to the disclosure;
   b) if the discloser wishes to remain anonymous, give the Authorised Officer their assessment of the risk of reprisal; and
   c) inform the discloser that they have given the information to an Authorised Officer and advise the discloser of the name and contact details of that Authorised Officer.

4.4 Where a supervisor receives an anonymous disclosure, the supervisor must refer it to an Authorised Officer as soon as is reasonably practicable.

4.5 Supervisors must treat disclosures with the highest degree of confidentiality at all times. For further information please refer to section 7-Confidentiality.

5. Procedures for Authorised Officers

5.1 Once an Authorised Officer has received a disclosure of suspected wrongdoing (either directly from a discloser, or via the discloser's supervisor), the PID Act requires certain steps to be taken.

Initial Assessment

5.2 When an Authorised Officer receives a disclosure of suspected wrongdoing, they must consider the disclosed information and decide whether it meets the criteria for an internal disclosure under the PID Act and whether they are an authorised internal recipient for that disclosure. An internal disclosure is made when:
- a person who is or has been a public official;
- discloses to an authorised internal recipient (supervisor, Authorised Officer or principal officer);
- the discloser believes on reasonable grounds that the information tends to show one or more instances of disclosable conduct.

5.4 If the Authorised Officer has reasonable grounds to believe that the discloser may be unaware of what the PID Act requires for the disclosure to be considered an internal disclosure, the Authorised Officer must:
- inform the discloser that the disclosure could be treated as an internal disclosure under the PID Act;
- explain to the discloser what the PID Act requires for a disclosure to be an internal disclosure;
- explain to the discloser the protections provided by the PID Act to persons who make disclosures under the Act;
- advise the discloser of any orders or directions that may affect disclosure of information; and
- advise the discloser that they should seek their own independent legal advice on the impact of the PID Act and their rights and responsibilities.

Ask the Discloser for consent

5.5 Where the Authorised Officer is aware of the contact details of the discloser, the Authorised Officer must, within 14 days after receiving the disclosure and before allocating the disclosure, ask the discloser whether he or she:
- consents to the Authorised Officer giving the discloser's name and contact detail/s to the principal officer or their delegate/s under the PID Act; and
- wishes the disclosure to be investigated.

5.6 The Authorised Officer must make a written record of the discloser's responses (if any) to the questions above at point 5.5. Where a discloser does not respond within 7 days to the question referred to above:
- the discloser is taken not to have consented to the disclosure of their name and contact details to the principal officer or their delegate/s; and
- the discloser is taken to wish the disclosure to be investigated.

Conduct preliminary inquiries

5.7 Under the PID Act, an Authorised Officer has the power to make any inquiries and obtain further information before making a decision about allocating the matter for investigation. Making preliminary inquiries is not the same as conducting an investigation. The Authorised Officer's task is to quickly assess the disclosed information to ascertain if anything more needs to be known before they can make an informed decision about:
- whether the disclosure is an internal disclosure under the PID Act;
- whether the Authorised Officer is an authorised internal recipient for that disclosure, based on the subject matter and/or whether the discloser belongs (or last belonged) to the Authorised Officer's agency (NIAA); and

- who the disclosure should be allocated to for handling (provided that the answers to the two preceding questions is 'yes').

Decision to allocate the disclosure

5.8 Once the Authorised Officer is satisfied that the disclosed information is an internal disclosure, they must allocate it for handling under the PID Act.

5.9 The Authorised Officer will use his or her best endeavours to decide the allocation within 14 days after the disclosure is made to the Authorised Officer.

5.10 The Authorised Officer may allocate the handling of the disclosure to one or more agencies, including the NIAA, the Ombudsman, the IGIS or an investigative agency prescribed by the PID Rules.

5.11 In deciding the agency, or agencies, to which a disclosure will be allocated, the Authorised Officer will have regard to the principle that the NIAA should only deal with disclosures that relate to the agency.

5.12 The Authorised Officer must not allocate a disclosure to another Commonwealth agency unless an Authorised Officer of that agency has consented to the allocation.

Decision not to allocate

5.13 If during the initial assessment the Authorised Officer is satisfied on reasonable grounds, that there is no reasonable basis on which the disclosure could be considered to be an internal disclosure, then the Authorised Officer may decide not to allocate the matter.

5.14 The basis on which an Authorised Officer could be satisfied of this includes:

- the disclosure has not been made by a person who is, or was, a public official;
- the disclosure was not made to an authorised internal recipient or supervisor;
- the disclosure is not about disclosable conduct;
- the person who is alleged to have carried out the disclosable conduct was not a public official at the time they are alleged to have carried out that conduct; and
- the disclosure is not otherwise a public interest disclosure within the meaning of the PID Act.

Inform relevant person of the allocation

5.15 Where an Authorised Officer decides that a disclosure is not to be allocated, they must, where the discloser's contact details are known to the Authorised Officer, advise the discloser in writing within 14 days that the disclosure is not to be allocated and inform the discloser of any other courses of action that might be available to the discloser under other laws of the Commonwealth.

5.16 Where an Authorised Officer decides to allocate a disclosure to the NIAA, they must as soon as reasonably practicable and within 14 days of the decision:

- inform the Principal Officer or their delegate/s of the allocation;
- inform the Commonwealth Ombudsman's Office (and use any prescribed forms established by the Ombudsman's office); and
- inform the discloser of the allocation (if the contact details of the discloser are known).

5.17 If the Authorised Officer allocates a disclosure to:

- an intelligence agency, the Authorised Officer will inform the IGIS of this in writing; or
- another agency, the Authorised Officer will inform the Commonwealth Ombudsman of this in writing.

5.18 The Authorised Officer need not notify the discloser of the decision to their allocation decision if it is not reasonably practicable to do so, i.e. if the discloser has not provided his contact details. If a decision is made that it is not reasonably practicable to notify the discloser, the Authorised Officer must record the reasons why this is the case.

Make a record of the allocation decision

5.19 When an Authorised Officer allocates the handling of a disclosure to one or more agencies, the Authorised Officer must keep an appropriate record of:

- the decision (including the name of each agency to which the disclosure is to be allocated);
- the reasons for the decision; and
- if the disclosure is allocated to another Commonwealth agency, the consent provided by the Authorised Officer of that agency.

5.20 In addition, the Authorised Officer must keep appropriate records of whether the discloser was informed of the allocation decision and, if so, of:

- the day and time the discloser was notified;
- the means by which the discloser was notified; and
- the content of the notification.

5.21 These records should be kept confidential and restricted to a need-to-know basis.

Conduct a risk assessment

5.22 Where an Authorised Officer allocates a disclosure, they must conduct a risk assessment based on a checklist of risk factors in consultation with Legal Services Branch. For further information refer to Appendix 1-Risk Assessment Information.

If necessary, develop a risk mitigation strategy

5.23 Where necessary, the Authorised Officer or the Principal Officer (or their delegate/s) will develop a strategy to mitigate the risk of reprisal action being taken against the discloser, which may involve support measures set out in 5.24 and 5.25.

Provide support for the Discloser and the person against whom a Disclosure is made

5.24 <u>Support for disclosers</u>

Regardless of the outcome of the risk assessment, the NIAA will take all reasonable steps to protect disclosers who have made a public interest disclosure from detriment or threats of detriment relating to the disclosure. This may include one or more of the following:

- appointing a support person to assist the discloser, who is responsible for checking on the wellbeing of the discloser regularly;
- informing the discloser of the progress of the investigation;

- where there are any concerns about the health and wellbeing of the discloser, liaising with the NIAA's work health and safety section; and/or
- transferring the discloser to a different area within the workplace or approving remote/teleworking (with the consent of the discloser). This is only likely to be appropriate in cases involving very major or extreme risk.

5.25 Support for persons against whom disclosure has been made

The NIAA will also take steps to support any employee who is the subject of a public interest disclosure. This may include one or more of the following actions:

- advising the employee of his or her rights and obligations under the PID Act and about the NIAA's investigation procedures, including the employee's rights to procedural fairness;
- informing the employee of the progress of the investigation as far as reasonably
- practicable;
- ensuring that the identity of the employee is kept confidential as far as reasonably practicable;
- where there are any concerns about the health and wellbeing of the employee, liaising with the NIAA's work health and safety section;
- transferring the employee to a different area within the workplace or approving remote/teleworking (with the consent of the employee). This is only likely to be appropriate in cases involving very major or extreme risk; and/or
- advising the employee that they should seek their own independent legal advice on the impact of the PID Act and their rights and responsibilities.

6. Procedures for Principal Officer / Delegates (Investigating Officer)

6.1 The CEO (the Principal Officer) has delegated all of his functions under the PID Act. If an Authorised Officer allocates a matter to the NIAA for determination, the Principal Officer or their delegate/s must follow a number of steps in accordance with the PID Act.

Initial advice to the Discloser about the investigation

6.2 The Principal Officer or their delegate/s must check whether the discloser has already been informed of the Principal Officer's powers to investigate the disclosure (refer to 5.5 – 5.6'. If not, that advice should be provided to the discloser within 14 days after receiving a disclosure from an Authorised Officer, including the estimated length of time to complete investigations under the PID Act (within 90 days of allocation).

Decision to investigate the disclosure or not

6.3 After receiving an allocation of a disclosure from an Authorised Officer, the Principal Officer or their delegate/s must ensure that, where it is reasonably practicable to do so, the discloser is informed, within 14 days, of whether or not the disclosure will be investigated.

6.4 However, the Principal Officer or their delegate/s may decide not to investigate the disclosure if:

- the discloser is not a current or former public official;
- the information does not, to any extent, concern serious disclosable conduct;
- the disclosure is frivolous or vexatious;

- the disclosure is the same or substantially the same as another disclosure which has been or is being investigated under the PID Act;
- the disclosure is the same or substantially the same as a disclosure that is currently being investigated under another Commonwealth law, and it would be inappropriate to conduct another investigation at the same time;
- the disclosure is the same or substantially the same as a disclosure that has already been investigated under another Commonwealth law, and the Principal Officer or their delegate/s is reasonably satisfied that there are no matters that warrant further investigation;
- the discloser has advised the Principal Officer or their delegate/s that they do not wish for the disclosure to be investigated or pursued, and the Principal Officer or their delegate/s is reasonably satisfied that there are no matters that warrant further investigation; or
- it is impracticable to investigate the disclosure because:
  - of the age of the information;
  - the discloser has not disclosed their name and contact details; or
  - the discloser has failed, or is unable, to give the Principal Officer or their delegate/s the information or assistance they requested.

6.5 If the investigation has already started, the Principal Officer or their delegate/s may subsequently decide to stop the investigation on one of the discretionary grounds set out above.

Notify the discloser and Ombudsman

6.6 If the Principal Officer or their delegate/s decides not to investigate a disclosure, they must as soon as reasonably practicable and within 14 days of the decision:
- inform the Ombudsman in writing of that decision and the reasons for that decision; and
- where they have been given the name and contact details of the discloser, inform the discloser of that decision, the reasons for that decision and of other courses of action that may be available to the discloser under other laws of the Commonwealth.

6.7 If the Principal Officer or their delegate/s decides to investigate the disclosure, they must inform the discloser as soon as reasonably practicable (unless already advised previously):
- the decision to investigate the disclosure; and
- of the estimated length of the investigation.

6.8 If the Principal Officer or their delegate/s decides to investigate a disclosure, but then decides not to investigate the disclosure further they must, as soon as reasonably practicable and within 14 days of the decision:
- inform the discloser in writing of that decision and the reasons for that decision; and
- inform the Commonwealth Ombudsman of that decision and the reasons for that decision.

Investigating the disclosure

6.9 If the Principal Officer or their delegate/s decides to investigate a public interest disclosure, they must investigate within 90 days and consider whether there are one or more instances of disclosable conduct.

General principles

6.10 The following general principles will apply to the conduct of investigations:
- Maintaining the confidentiality of the identity of the discloser.
- The investigation will be conducted in accordance with the principles of procedural fairness.

- A person who is the subject of the investigation will have an opportunity to respond or provide information.
- In the event that an interview is to be conducted:
    - it will be conducted in a manner consistent with the *Public Interest Disclosure Standard 2013,* and
    - the person being interviewed will be offered the opportunity to have a suitable support person present during the interview.
- A decision on whether evidence is sufficient to prove a fact will be determined on the balance of probabilities.

6.11 Aside from compliance with the abovementioned principles, the Principal Officer and their delegate/s are free to conduct the investigation as they see fit. The way in which the investigation is conducted may vary depending on the alleged conduct which is being investigated. In particular, where the Principal Officer or their delegate/s consider that the nature of the disclosure is such that the outcome of the investigation is likely to be referral of the matter for investigation under another process or procedure, the investigation will be conducted in accordance with those other established processes or procedures.

Obtaining information

6.12 The starting point of an investigation is the information provided by the discloser. However, the Principal Officer and their delegate/s may also consider whether the information they obtain during the investigation indicates that there are other, or different instances of disclosable conduct.

6.13 During the investigation, the Principal Officer or their delegate/s may, for the purposes of the investigation, obtain information from such person/s and make such inquiries as they see fit.

6.14 When conducting interviews as part of an investigation, an interviewee will be informed of the following:

- The identity and function of each individual conducting the interview.
- The process of conducting an investigation.
- The authority of the Principal Officer (and relevant delegate/s) under the PID Act to conduct the investigation.
- The protections provided to witnesses under section 57 of the PID Act.
- The interviewee's duty:
    - if they are a public official - to use their best endeavours to assist the Principal Officer or their delegate/s in the conduct of an investigation under the PID Act (subject to the public official's privilege against incriminating themselves or exposing themselves to a penalty);
    - not to take or threaten to take reprisal action against the discloser; and
    - subject to the PID Act, not to disclose the identity of the person who made the disclosure.

6.15 The Principal Officer or their delegate/s will ensure:

- an audio and/or visual recording of the interview is not made without the interviewee's knowledge;
- when the interview ends, the interviewee is given an opportunity to make a final statement or comment or express a position; and
- any final statement, comment or position by the interviewee is included in the record of the interview.

6.16 In conducting the investigation, the Principal Officer or their delegate/s may adopt findings set out in reports of investigations or inquiries under other Commonwealth laws or executive powers, or other investigations under the PID Act.

Referral of information to police

6.17 If, during the course of the investigation, the Principal Officer or their delegate/s suspect on reasonable grounds that some of the information disclosed or obtained in the course of the investigation is evidence of the commission of a criminal offence, the Principal Officer may disclose the information to a member of an Australian police force. If the information relates to a criminal offence that is punishable for a period of at least two years, the Principal Officer must disclose the information to a member of an Australian police force.

Procedural fairness

6.18 Procedural fairness does not require that a person, against whom allegations are made, must be advised as soon as the disclosure is received or as soon as an investigation is commenced.

6.19 Procedural fairness does require that the person, against whom allegations are made, is entitled to know the substance of allegations against them if that might result in an adverse finding being made about their conduct.

6.20 Procedural fairness does not equate to a right to know the identity of the discloser who has alleged that the person has committed wrongdoing. However, the person may be able to guess the discloser's identity because the substance of the allegations makes it evident.

6.21 Where the Principal Officer or their delegate/s, in preparing the investigation report, propose to:

- make a finding of fact; or
- express an opinion that is adverse to the discloser, to a public official who is the subject of the disclosure or to another person,

they must give the person who is the subject of that proposed finding or opinion a copy of the evidence that is relevant to that proposed finding or opinion and must give the person a reasonable opportunity to comment on it.

NOTE: The above paragraph will not apply where the investigation does not make substantive findings or express adverse opinions but instead simply recommends or decides that further investigation action should or should not be taken or will or will not be taken.

6.22 The Principal Officer or their delegate/s must ensure that a finding of fact in a report of an investigation under the PID Act is based on logically probative and relevant evidence.

Time limits

6.23 The Principal Officer and his delegate/s have 90 days from the date the disclosure was allocated in which to complete the investigation.

6.24 It is possible to seek one or more extensions of time from the Ombudsman. A request to the Ombudsman for an extension of time must be made at least 21 days prior to the expiry of the

investigation completion date. The application for extension should include reasons why the investigation cannot be completed within the time limit, the views of the discloser and an outline of action taken to progress the investigation.

6.25 An investigation that is not completed within the specified time limit does not mean that the investigation becomes invalid.

Prepare investigation report

6.26 Once the Principal Officer or their delegate/s has completed the investigation, they must prepare a report of the investigation.

6.27 A report of an investigation under the PID Act must set out:
- the matters considered in the course of the investigation;
- the duration of the investigation;
- the investigator's findings (if any);
- the action (if any) that has been, is being or is recommended to be taken; and
- any claims made about, and any evidence of, detrimental action taken against the discloser, and the NIAA's response to those claims and that evidence.

6.28 Where relevant, a report must:
- identify whether there have been one or more instances of disclosable conduct;
- identify any regulations, rules, administrative requirements or similar matters to which the disclosable conduct (if any) relates;
- explain the steps taken to gather evidence;
- set out a summary of the evidence; and
- set out any findings and recommendations made based on that evidence.

6.29 If the Principal Officer or their delegate/s consider that information disclosed in the course of a public interest disclosure may be appropriately dealt with under another NIAA procedure or policy, they may recommend in the investigation report that this occur.

Refer recommendations to Principal Officer / Appropriate delegate

6.30 If the investigation report contains recommendations in relation to instances of disclosable conduct, the recommendations must be referred to the Deputy CEO or the NIAA Chief Operating Officer, as delegates of the Principal Officer to ensure appropriate action is taken.

Provide report to Discloser

6.31 The Principal Officer or their delegate/s must, within a reasonable time of preparing a report of an investigation under the PID Act, give a copy of the report to the discloser.

6.32 The Principal Officer or their delegate/s may delete from the copy of the report given to the discloser any material:
- that is likely to enable the identification of the discloser or another person; or
- the inclusion of which would result in the copy being a document;
- that is exempt for the purposes of Part IV of the *Freedom of Information Act 1982;* or
- having, or being required to have, a national security or other protective security classification; or
- containing intelligence information.

6.33 The Principal Officer or their delegate/s must delete from the copy of a report given to the discloser any material which would result in the report contravening a designated publication restriction.

7. Confidentiality

7.1 Disclosures should be assessed and investigated discreetly, with a strong emphasis on maintaining confidentiality of both the discloser and any person who is the subject of the disclosure. It is an offence for a person who has information obtained in the course of conducting a disclosure investigation, or in connection with their powers and functions under the PID Act, to disclose or use this information.

7.2 Any email correspondence between supervisors, Authorised Officers and/or the Principal Officer (or their delegate) should include in the subject line 'For Addressee Eyes Only- Public Interest Disclosure'. This alerts any support staff who may have access to emails that this email is not to be opened.

7.3 Any interviews conducted by an Authorised Officer, the Principal Officer or their delegate/s should be conducted in private.

7.4 Any interviews with the discloser should be arranged so as to avoid the identification of the discloser by other staff of NIAA.

7.5 Supervisors, managers and Authorised Officer who seek further advice from the NIAA's Legal Services Branch regarding a disclosure must de-identify the information. When referring to involved parties they should be referred to as the 'discloser' and the 'subject person'.

8. Record Keeping

8.1 Where an Authorised Officer is required to keep a record under this procedure, the record may be kept in hard copy or in an electronic form or in both. Access to these records must be restricted to the Authorised Officer, the Principal Officer (or their delegate/s) or other employees in the NIAA who require access in order to perform some function under the PID Act or for the purposes of another law of the Commonwealth (for example, under the *Work Health and Safety Act 2011* or the *Public Service Act 1999).*

8.2 When a person ceases their role as an Authorised Officer at the NIAA (including because of their resignation or movement to another agency), they must transfer all records relating to public interest disclosures to another Authorised Officer within the NIAA.

9. Monitoring and Evaluation

9.1 Each Authorised Officer must provide a six monthly report to the Primary Delegate (a person being a Principal Lawyer in the Legal Services Branch who will facilitate the Agency reporting to the Commonwealth Ombudsman) specifying the number of public interest disclosures received by the Authorised Officer and the nature of the disclosable conduct for each disclosure (by reference to the relevant item or paragraph in the definition). The report must also include any

disclosures that have been allocated to the NIAA by another Commonwealth agency's Authorised Officer.

9.2 The Primary Delegate will collate the NIAA's report to the Ombudsman on disclosures made during the financial year.

9.3 Each delegate of the Principal Officer must advise the Primary Delegate of every decision made by the delegate to investigate a disclosure during the financial year.

9.4 Each delegate of the Principal Officer who takes action in response to a recommendation made in an investigation report must inform the Primary Delegate of the action taken.

9.5 The Primary Delegate must prepare the NIAA's report for the Principal Officer's consideration within the time specified by the Principal Officer.

9.6 The Principal Officer will send the NIAA's report to the Ombudsman within the time requested by the Ombudsman or as otherwise agreed with the Ombudsman.

10. Resources

10.1 Advice

More advice concerning these procedures and other workplace conflict and ethical dilemma situations can be obtained by contacting the area responsible for PID administration via email at: PID@niaa.gov.au.

10.2 Useful websites

Commonwealth Ombudsman
https://www.ombudsman.gov.au

Australian Public Service Commission
www.apsc.gov.au

APPENDIX l - RISK ASSESSMENT INFORMATION

Extract: Agency Guide to the *Public Interest Disclosure Act* 2073 (April 2016. Version 2)

Preventing and Protecting from Detriment and Reprisal

The Principal Officer of each agency must take reasonable steps to protect public officials who belong to their agency from detriment, or threats of detriment relating to disclosures (s 59(3)(a)). This protection obligation extends beyond the officials making disclosures. The Principal Officer is also obliged to protect witnesses and other officials who may be suspected to have made a disclosure, and officials who are the subject of allegations.

What is detriment and reprisal?

Detriment

'Detriment' includes any disadvantage to a person, including dismissal, injury in their employment, discrimination between them and other employees or alteration of their position to their disadvantage (s 13(2)). For example, it could include an omission or action (or threat of action) that results in:

- a physical or psychological injury, including a stress-related injury
- intimidation, harassment or victimisation
- loss or damage to property
- disadvantage to a person's career (for example, denying them a reference or a promotion without appropriate reasons).

What is reprisal?

Reprisal occurs if someone causes, by an act or omission, any detriment to another person because they believe or suspect that person, or anyone else, may have made or intends to make a public interest disclosure (s 13(1)).

What is not a reprisal?

Administrative action that is reasonable to protect the discloser from detriment is not a reprisal (s 13(3)). For example, where a person has made a disclosure in relation to practices in their immediate work area, it may be appropriate to transfer them to another work area to ensure they are not harassed or victimised. It is important to ensure there is no perception that they are being punished for having made a disclosure.

Making a disclosure also does not exclude the discloser from reasonable management action for any unsatisfactory performance or wrongdoing on their part - such action is not a reprisal.

Risk assessment procedures

Each agency must establish procedures for assessing risks that reprisal may be taken against people making public interest disclosures (s 59(1)). Those procedures must also outline what support will be made available to public officials who make disclosures (s 7 of the PID Standard).

Given that the obligation to protect officials from detriment extends beyond disclosers, agencies should also consider including in their procedures information about support and assessing risks for

others who may be at risk of reprisal and detriment because of a public interest disclosure. That would include witnesses, other staff who might be suspected to have made disclosures, and any official who is the subject of any allegation.

A risk assessment involves assessing the specific behaviour and circumstances that may result in reprisals. Once those risks have been assessed, and the likelihood of them occurring, the agency needs to consider appropriate strategies to prevent or contain them. Inappropriate workplace behaviour, including harassment, intimidation, undermining of authority, ostracism, humiliation, questioning of motives and heavier scrutiny of work can greatly increase stress and can result in serious injury to someone who has made a disclosure. The risk assessment can include not only the risk of direct reprisal against the discloser, but also the risk of related workplace conflict or difficulties.

An accurate and objective risk assessment allows the agency to put suitable strategies in place to control the risks and defend itself against any allegations of having failed to protect a discloser.

When should a risk assessment be done?

An initial risk assessment should be completed as soon as possible after a disclosure is received, or after the agency is notified that a disclosure concerning their agency has been received (for example, if the Ombudsman, IGIS or investigative agency decides to investigate a disclosure made directly to them). This gives the agency the best chance of recognising any risk of reprisals or associated workplace conflict.

The risk of reprisal may increase or change as the PID investigation progresses, and more people become aware of the disclosure. Even after the investigation has been completed, the risk of reprisal may persist, or even increase, particularly if action has been recommended to address the investigation findings. It is therefore necessary for agencies to reassess the risk assessment when things change, and document the updated assessment and any action to be taken.

Who should conduct a risk assessment?

The PID Act requires the Principal Officer to establish procedures for assessing the risk of reprisal in relation to public interest disclosures. Those procedures should clearly identify who is responsible for conducting the risk assessment. Given that the initial risk assessment should be done as soon as possible after a disclosure has been received, it may be appropriate for the Authorised Officer to conduct that initial assessment. Alternatively, it could be the responsibility of the Authorised Officer to ensure that information is passed to another officer with requisite skills and experience to conduct the risk assessment.

The responsible officer, determined according to an agency's procedures, should conduct their risk assessment based on a checklist of risk factors, and make records of their assessment. See 8.5.4 of the Commonwealth Ombudsman’s guide for a suggested risk assessment framework.

Who should be consulted?

The best sources of information about potential risks are people who are involved in the particular workplace, especially the discloser and their supervisor or manager (provided that person is not involved in the alleged wrongdoing).

Asking the discloser why they are reporting wrongdoing and who they might fear a reprisal from can be helpful in:

- assessing likely perceptions amongst staff as to why the discloser came forward and how colleagues may respond if the discloser's identity becomes known;
- managing the discloser's expectations about how other staff might perceive their disclosure;
- reducing the potential for future conflict between the discloser and management about whether effective support was provided; and
- identifying the motives of staff allegedly involved in reprisals if a later investigation becomes necessary.

The supervisor or manager may also be a valuable source of information about these matters.

Risk assessments for anonymous disclosers

If an anonymous disclosure is made, it may be difficult for an agency to protect the discloser and other staff from reprisal or workplace conflict. However, a risk assessment should still be conducted where an anonymous disclosure is received, to assess whether the discloser's identity can be readily ascertained or may become apparent during an investigation.

Staff may speculate, correctly or otherwise, about who made the disclosure, and that person may be at risk of reprisal. If the discloser's identity becomes known, the risk of reprisal may escalate and require prevention or mitigation strategies to be implemented, such as raising the issue with staff, reminding them of the agency's commitment to the public interest disclosure process and reminding them that reprisal is a criminal offence.

Risk assessment framework

Agencies may have their own well developed processes for assessing risks. However, the following framework is suggested for consideration. It entails four steps:

- Identifying - are there reprisals or related workplace conflict problems in the workplace, or do they have the potential to be problems?
- Assessing - what is the likelihood and consequence of reprisals or related workplace conflict?
- Controlling - what strategies should be put in place to prevent or contain reprisals or related workplace conflict?
- Monitoring and reviewing - have the strategies been implemented and were they effective?

Identifying risks

The agency should develop a list of risk factors that can alert those dealing with the PID, and managers, to problems. Table 1 below includes some indicators of a higher risk of reprisals or workplace conflict.

The person doing the risk assessment should clearly define the individual factors affecting the particular discloser/official and the specific workplace when assessing if there are factors that make reprisals or related workplace conflict likely. Table 2 is a risk matrix that lists the types of detriment that might occur in NIAA's work environment.

Assessing risks

The person assessing the risk should consider:

- the likelihood of reprisals or related workplace conflict occurring - this may be high if:

    - there have already been threats
    - there is already conflict in the workplace
    - a combination of circumstances and risk factors indicate reprisals or related workplace conflict are likely.
- the potential consequences if the risks eventuate, both to the discloser's immediate and long term wellbeing and the cost to the agency.

Controlling risks

The agency should plan and implement strategies to control the risks likely to expose a discloser to reprisals or related workplace conflict. The discloser should be consulted about possible strategies.

If the risk is assessed as sufficiently high, the agency should prepare a plan to prevent and contain reprisals against the discloser or related workplace conflict. If it has been determined that a discloser will require support, the agency should develop a strategy for providing an appropriate level of support, such as appointing a support person.

If the discloser's identity is likely to be known or become known in their workplace, the agency should adopt a proactive approach, for example, by raising the matter with staff, reiterating the agency's commitment to encouraging and where appropriate investigating public interest disclosures, and reminding staff that taking or threatening a reprisal is a criminal offence.

Monitoring and reviewing risks

Problems in the workplace can arise at any point after a disclosure has been made, including during an investigation, and afterwards, when action is being taken to address any findings. The risk assessment should be monitored and reviewed as necessary, including by checking with the discloser to see if reprisals have been made or threatened. Records should be made whenever the risk assessment is reviewed or revised.

TABLE 1 - INDICATORS OF A HIGHER RISK OF REPRISALS OR WORKPLACE CONFLICT

Threats or past experience	○ Has a specific threat against the discloser been made? ○ Is there a history of conflict between the discloser and the subjects of the disclosure, 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? ○ Has the discloser already raised the substance of the disclosure or revealed their identity in the workplace? ○ Is the discloser's immediate work unit small? ○ Are there circumstances, such as the discloser's stress level, that will make it difficult for them to not 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 maintain confidentiality?
Significant reported wrongdoing	○ Are there allegations about individuals in the disclosure? ○ Who are their close professional and social associates? ○ Is there more than one wrongdoer involved in the matter? ○ Is the reported wrongdoing serious? ○ Is or was the reported wrongdoing occurring frequently? ○ Is the disclosure particularly sensitive or embarrassing for any subjects of the disclosure, senior management, the agency or 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 officer? ○ 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 the organisation?

TABLE 2 - RISK ASSESSMENT MATRIX

	Identified risk event	**Likelihood High/Medium/Low**	**Consequence Serious/Moderate/ Minor**	**Action to mitigate Yes/No – (if yes, describe)**
1	Assault			
2	Verbal assault			
3	Stalking			
4	Cyber-bullying			
5	Silent treatment in workplace			
6	Interference to personal items			
7	Excluded from legitimate access to information			
8	Excluded from promotion			
9	Excluded from workplace sanctioned social events			
10	Unjustified change to duties/hours of work			
11	Dismissal			
12	Unjustified refusal of leave			
13	Onerous/unjustified audit of access to ICT/Time sheets			
14	Onerous/unjustified audit of expenditure of Commonwealth money/Cab charge use			
15	Other (describe)			