

Our ref: A2238253

// April 2022

Mr Sean Coley
Committee Manager of Integrity and Oversight Committee
Parliament of Victoria, Spring Street
EAST MELBOURNE VIC 3002

Dear Mr Coley

Witness welfare management during integrity agency investigations

Thank you for your letter dated 10 March 2022 seeking my Office's input to your Committee's inquiry into integrity agencies' management of the welfare of witnesses and others involved in agency investigations.

I would like to take the opportunity to outline the role of my Office in relation to witnesses and highlight some of our activities and materials that may assist your inquiry.

The *Ombudsman Act 1976* (the Ombudsman Act) sets out the functions and powers of my Office. We are responsible for investigating complaints from individuals, groups or organisations about the administrative actions of Australian government agencies, as well as some private sector organisations. Where we investigate complaints or undertake an own motion investigation, we seek information from agencies, rather than requesting or compelling information from individual agency staff.

Whilst the Ombudsman Act gives me wide-ranging powers to compel a person to produce information relevant to an investigation (including providing documents or attending as a witness to answer questions) in practice my Office rarely relies on those powers. Rather, where we investigate an agency, we generally direct written questions to the agency itself and obtain relevant information from the agency voluntarily. Occasionally we will provide agencies with a notice upon their request, as this is sometimes preferred by the agency.

My Office does not compel members of the public to provide information. We receive information from members of the public who contact us of their own volition. As such, we do not consider these people witnesses. Instead, we regularly engage with:

- complainants through our complaint handling function
- disclosers through the *Public Interest Disclosure Act 2013*, and
- reporters through our Defence abuse function under the *Ombudsman Regulations 2017*.

We publish materials setting out our approach to people who contact our Office. In particular, we would like to highlight the following:

- Information on our website about reporting abuse in Defence is located here at [Reporting abuse in Defence - Commonwealth Ombudsman](#). The dedicated webpage provides

information about our reporting process and frequently asked questions for potential reportees, including our approach to liaison with reportees.

- Section 8.6 of our Office's 'Agency Guide to the *Public Interest Disclosure Act 2013*', provided at **Attachment A**.
- Our Guidance for Complaint Handlers on dealing with risks of harm, provided at **Attachment B**.

I trust this information is useful. If you require further information from our Office, you or your staff are welcome to contact my officers at strategy@ombudsman.gov.au.

Yours sincerely



Penny McKay
Acting Commonwealth Ombudsman

Influencing systemic improvement in public administration



AGENCY GUIDE TO THE
PUBLIC INTEREST DISCLOSURE ACT 2013

April 2016
Version 2

Contents

FOREWORD	VIII
1 INTRODUCTION	1
2 HOW THE PUBLIC INTEREST DISCLOSURE SCHEME WORKS	2
2.1 THE PURPOSE OF THE PID ACT	2
2.2 WHAT IS A PUBLIC INTEREST DISCLOSURE?	2
Figure 1 – What is an internal public interest disclosure	3
2.3 WHO CAN MAKE A PUBLIC INTEREST DISCLOSURE?	4
2.3.1 Public officials	4
2.3.2 ‘Deemed’ public officials	4
2.4 PRIVATE INTEREST vs PUBLIC INTEREST	5
2.5 WHAT CAN BE DISCLOSED?	5
2.5.1 Whose conduct?	5
2.5.1.1 What is an ‘agency’?	5
2.5.1.2 Who is a ‘public official’?	6
2.5.1.3 What is a contracted service provider for a Commonwealth contract?	6
2.5.2 What kinds of disclosable conduct are covered by the PID Act?	7
2.5.3 Time limits for making a disclosure	8
2.6 WHAT IS NOT DISCLOSABLE CONDUCT?	8
2.7 WHO CAN A PUBLIC INTEREST DISCLOSURE BE MADE TO?	9
2.7.1 Internal disclosure to the agency concerned	9
2.7.1.1 Who is an authorised officer for an agency?	9
2.7.1.2 Making an internal disclosure to a supervisor	9
2.7.2 Internal disclosure to the Ombudsman or the IGIS	10
2.7.3 Internal disclosure to a prescribed investigative agency	10
2.7.4 Complaint to the Ombudsman or the IGIS	10
2.7.5 Disclosures to other people – emergency and external disclosures	10
2.7.5.1 Intelligence information and sensitive law enforcement information	11
2.7.5.2 Does an agency have to investigate an emergency or external disclosure?	11
2.7.6 Emergency disclosure	11
2.7.7 External disclosure	12
2.7.7.1 When is an investigation or subsequent action inadequate?	12
2.7.7.2 What is ‘contrary to the public interest’?	13
2.7.8 Disclosures to other people - legal practitioner disclosure	14
2.8 WHAT HAPPENS IF INFORMATION IS DISCLOSED OUTSIDE THESE CIRCUMSTANCES?	14
3 AGENCY OBLIGATIONS	15
3.1 WHY PUBLIC INTEREST DISCLOSURES ARE IMPORTANT	15
3.2 PRINCIPAL OFFICER RESPONSIBILITIES	16
3.2.1 Appointing authorised officers and ensuring that officials can contact them	16
3.2.2 Establishing agency PID procedures	17

3.2.3	Fostering agency culture	18
3.2.4	Staff awareness and training	19
3.2.4.1	Training	20
3.3	OTHER KEY PID ROLES AND RESPONSIBILITIES	20
3.3.1	Authorised officer responsibilities	20
3.3.2	Manager and supervisor responsibilities	21
3.3.3	All staff responsibilities	22
4	RECEIVING INTERNAL DISCLOSURES	23
4.1	RECEIVING AN INTERNAL DISCLOSURE FROM A PUBLIC OFFICIAL	23
4.1.1	A current or former public official	23
4.1.2	A 'deemed' public official	23
4.1.3	Who can receive a public interest disclosure?	23
4.1.4	How can a public interest disclosure be made?	24
4.1.5	Can a discloser be anonymous or use a pseudonym?	24
4.2	WHAT INFORMATION SHOULD THE DISCLOSER PROVIDE?	26
4.2.1	Information about the suspected wrongdoing	26
4.2.2	Is the discloser's motive relevant?	26
4.3	PROTECTION FOR THE DISCLOSER	27
4.4	THE DISCLOSER'S OBLIGATIONS	27
Figure 2 – Handling an internal disclosure under the PID Act		28
		28
5	INITIAL ASSESSMENT AND ALLOCATION UNDER THE PID ACT	29
5.1	INITIAL ASSESSMENT OF THE DISCLOSURE	29
5.1.1	Determining if the information is an internal disclosure	29
5.1.2	Does the information tend to show disclosable conduct?	29
5.1.2.1	Belief on reasonable grounds	29
5.1.2.2	Tends to show	30
5.1.3	Preliminary inquiries	31
5.2	ALLOCATION UNDER THE PID ACT	31
5.2.1	Which agency should a disclosure be allocated to?	31
5.2.2	Allocation to more than one agency	32
5.2.3	Who needs to consent to the allocation?	32
5.2.4	Can subsequent allocations be made?	32
5.2.5	Giving notice of the allocation	32
5.2.5.1	Informing the principal officer of the allocation	33
5.2.5.2	Informing the Ombudsman or IGIS of the allocation	33
5.2.5.3	Informing the discloser of the allocation decision	33
5.2.6	What records must the authorised officer make of their allocation?	34
5.2.6.1	What if the authorised officer cannot contact the discloser?	34
5.3	CONDUCTING AN INITIAL RISK ASSESSMENT	34
5.3.1	Protection of the discloser's identity	34
6	DECIDING WHETHER TO INVESTIGATE UNDER THE PID ACT	36

6.1	GENERAL REQUIREMENT TO INVESTIGATE A DISCLOSURE	36
6.1.1	Advising the discloser about the principal officer's powers	36
6.2	WHEN CAN AN AGENCY DECIDE NOT TO INVESTIGATE?	36
6.2.1	The discloser is not a public official	37
6.2.2	The disclosed information does not concern serious disclosable conduct	37
6.2.2.1	What is serious disclosable conduct?	37
6.2.3	What is meant by frivolous or vexatious?	38
6.2.4	Prior or current investigation of same matter	39
6.2.4.1	Investigated under the PID Act	39
6.2.4.2	Investigated under another law of the Commonwealth or the Commonwealth's Executive power	39
6.2.4.3	What sorts of investigations can be conducted under other Commonwealth laws?	39
6.2.5	The discloser does not want an investigation	40
6.2.6	Investigation of the disclosure is impracticable	40
6.2.6.1	Discloser's name and contact details unknown	40
6.2.6.2	Discloser unable or unwilling to assist in the investigation	41
6.2.6.3	The age of the information	41
6.3	DOES A DECISION NOT TO INVESTIGATE PREVENT OTHER ACTION?	41
6.4	WHAT RECORDS MUST BE MADE OF A DECISION NOT TO INVESTIGATE?	42
6.5	WHO MUST BE NOTIFIED OF A DECISION NOT TO INVESTIGATE?	42
6.5.1	Notifying the discloser	42
6.5.1.1	What if the discloser cannot be contacted?	43
6.5.2	Notifying the Ombudsman or IGIS	43
7	CONDUCTING AN INVESTIGATION	44
7.1	GENERAL REQUIREMENT TO INVESTIGATE AN INTERNAL DISCLOSURE	44
7.1.1	Initial advice to the discloser about the investigation	44
7.2	WHAT SORT OF INVESTIGATION IS REQUIRED?	44
7.2.1	Investigations under a separate investigative power	45
7.2.1.1	What is a separate investigative power?	45
7.2.1.2	Effect of using a separate investigative power	45
7.2.1.3	Notifying the discloser of the decision to investigate under a different law	45
7.3	INVESTIGATIONS UNDER THE PID ACT	45
7.3.1	What does it mean to 'investigate' under the PID Act?	45
7.3.2	Who should investigate?	46
7.3.2.1	Delegating the investigative function to a contractor	46
7.3.3	PID investigation requirements	46
7.3.3.1	Time limit for investigations	47
7.3.3.2	An administrative investigation	47
7.3.3.3	PID Standards for conducting investigations	47
7.3.3.4	What legal power does the investigator have to obtain information?	48
7.3.3.5	Interviewing a witness (including the discloser)	48

7.3.3.6	Standard of proof	49
7.3.3.7	Evidence	49
7.3.3.8	Procedural fairness	50
7.3.3.9	What must the official who is the subject of the disclosure be told?	50
7.3.3.10	Ensuring confidentiality of the investigation	51
7.3.4	Is a different type of investigation appropriate?	51
7.3.4.1	Investigation of alleged fraud	52
7.3.4.2	Investigation of disclosure about a possible breach of a Code of Conduct	52
7.3.5	PID investigation report	53
7.3.5.1	Detrimental action against the discloser	54
7.3.5.2	Findings of fact	54
7.3.5.3	Copy for the discloser	54
7.3.6	Criminal matters	54
7.3.6.1	Notifying the police	54
7.3.7	What impact can investigations have on the workplace?	55
7.4	AFTER THE INVESTIGATION	55
7.4.1	What should a person be told if allegations were made against them?	55
7.4.2	What action does an agency need to take?	56
7.4.3	What happens if the disclosure is not substantiated?	56
7.4.4	What if the discloser is not satisfied with the agency's action?	56
7.5	SOME ADMINISTRATIVE CONSIDERATIONS	57
7.5.1	Keeping the discloser informed	57
7.5.2	Keeping records	58
7.5.3	Freedom of Information requests	58
7.5.4	Monitoring and evaluation	58
8	SUPPORT AND PROTECTION UNDER THE PID ACT	60
8.1	CONFIDENTIALITY	60
8.2	PROTECTION FOR THE DISCLOSER	61
8.2.1	Protecting the discloser's identity	61
8.2.1.1	Measures to protect the discloser's identity	62
8.2.1.2	Can the discloser's identity be revealed to a court or tribunal?	63
8.2.2	Discloser's immunity from liability for making a disclosure	63
8.2.2.1	Can immunity from disciplinary action be granted?	64
8.2.2.2	What happens if proceedings are commenced?	64
8.3	PROTECTION FOR WITNESSES IN A PID INVESTIGATION	64
8.3.1	Witness's immunity from liability for providing information	64
8.3.1.1	What if the witness wants to raise other matters?	65
8.4	OFFICIALS EXERCISING POWERS OR PERFORMING FUNCTIONS UNDER THE PID ACT	65
8.5	PREVENTING AND PROTECTING FROM DETRIMENT AND REPRISAL	65
8.5.1	What is detriment and reprisal?	66
8.5.1.1	Detriment	66

8.5.1.2	What is reprisal?	66
8.5.1.3	What is not a reprisal?	66
8.5.1.4	Managing the discloser’s performance	66
8.5.2	Reprisal protections in the PID Act	67
8.5.3	Risk assessment procedures	67
8.5.3.1	When should a risk assessment be done?	67
8.5.3.2	Who should conduct a risk assessment?	67
8.5.3.3	Who should be consulted?	68
8.5.3.4	Risk assessments for anonymous disclosers	68
8.5.4	Risk assessment framework	68
8.5.4.1	Identifying risks	69
8.5.4.2	Assessing risks	69
8.5.4.3	Controlling risks	69
8.5.4.4	Monitoring and reviewing risks	69
8.6	PRACTICAL SUPPORT AND PROTECTION STRATEGIES	72
8.6.1	Support for the discloser	72
8.6.2	What are the ongoing support requirements?	72
8.6.3	How can an agency protect an official from reprisal?	73
8.7	ACCESS TO COURT	73
8.7.1	Federal Court and Federal Circuit Court	73
8.7.1.1	Injunctions, apologies and other orders	74
8.7.1.2	Compensation	74
8.7.1.3	Reinstatement	74
8.7.2	Fair Work Commission	74
8.8	REPRISAL IS A CRIME	74
9	THE ROLE OF KEY AGENCIES	76
9.1	OMBUDSMAN	76
9.1.1	Determining standards	76
9.1.2	Receiving and allocating disclosures	76
9.1.3	When will the Ombudsman investigate a disclosure?	77
9.1.4	Making decisions about extensions of time	77
9.1.3	When will the Ombudsman investigate a disclosure?	78
9.1.4	Making decisions about extensions of time	78
9.1.5	Providing assistance, education and awareness programs	79
9.1.6	Preparing annual reports	79
9.1.7	Assisting the Ombudsman	79
9.2	INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY	80
9.2.1	IGIS: receiving, allocating and investigating	80
9.3	PRESCRIBED INVESTIGATIVE AGENCIES	80
	APPENDIX 1 – FURTHER INFORMATION	81

Foreword

I am very pleased to publish the second edition of the Commonwealth Ombudsman's Agency Guide to the *Public Interest Disclosure Act 2013* (the PID Act).

The Commonwealth Ombudsman and the Inspector-General of Intelligence and Security (IGIS) have important roles in the PID Scheme. The Ombudsman, in consultation with the IGIS, issued the *Public Interest Disclosure Standard 2013* (the PID Standard) which sets out procedures that agencies must comply with when dealing with disclosures. The Ombudsman's office works co-operatively with agencies to help resolve any issues arising from the implementation of the scheme, and to provide guidance on its operation. The IGIS performs this function in relation to intelligence agencies. The Ombudsman is also responsible for promoting awareness and understanding of the PID Act, and for monitoring and reporting to Parliament each year about the operation of the PID scheme.

In December 2013, my office released the first edition of the *Agency Guide to the Public Interest Disclosure Act 2013*. The guide was intended to promote consistent implementation of the PID Act across the public sector. It explained how the PID Act was designed to work, set out the statutory obligations for agencies and suggested best practice for handling public interest disclosures, once the PID Act commenced on 15 January 2014.

This second edition of the *Agency Guide to the Public Interest Disclosure Act 2013* has been extensively revised and expanded to incorporate what we have learned through our practical experience of the PID Act over its first two years of operation. I have been impressed with the enthusiasm and cooperation that agencies have shown in implementing the public interest disclosure scheme to date. Hopefully, agencies will use this guide to refresh their understanding of the scheme and to check that their policies and procedures meet all requirements under the PID Act and the PID Standard.

We have developed and published on our website a range of fact sheets and promotional materials about the PID scheme. We convene and support a network of Communities of Practice for agency staff in Australian capital cities to meet and share information about the PID scheme. In conjunction with the Ombudsman for NSW and the Queensland Ombudsman, we host the Whistling Wiki, which is a closed online community for Australian PID practitioners.

More information about my office's PID education and resources is available on our website at www.pid.ombudsman.gov.au.

I encourage agencies to continue to use my office as a source of information and support in meeting their PID obligations. Your questions and feedback help us to ensure better practice in dealing with public interest disclosures.



Colin Neave
Commonwealth Ombudsman

Contact the Ombudsman's PID Team:

Telephone: 02 6276 3777
Email: pid@ombudsman.gov.au
Post: GPO Box 442
Canberra ACT 2601

1 Introduction

This guide has been developed to assist Commonwealth agencies fulfil their obligations under the *Public Interest Disclosure Act 2013* (PID Act) and *Public Interest Disclosure Standard 2013* (PID Standard).

The guide has nine chapters:

- 1 *Introduction* – explains the guide’s structure and the relevant legislation
 - 2 *How the PID scheme works* – outlines the scope and elements of the public interest disclosure scheme
 - 3 *Agency obligations* – sets out the need for strong agency commitment to encourage reporting of wrongdoing and take appropriate action, and identifies the responsibilities of key agency staff
 - 4 *Receiving internal disclosures* – sets out how disclosures should be encouraged and received
 - 5 *Allocating disclosures for handling under the PID Act* – discusses how disclosures are allocated for investigation
 - 6 *Assessing whether to investigate* – explains key considerations in deciding whether to investigate, and what happens if an agency decides not to investigate under the PID Act
 - 7 *Conducting an investigation* – discusses agency obligations regarding the conduct of investigations including procedural fairness, investigation reports and notification requirements
 - 8 *Support and protection* – discusses how disclosers are protected under the PID Act and avenues for assistance.
 - 9 *The role of key agencies* – sets out the role of the Ombudsman, the Inspector-General of Intelligence and Security (IGIS) and prescribed investigative agencies
- Appendix 1* – Other matters – provides further information

This guide refers, where relevant, to provisions of the PID Act and PID Standard (made by the Commonwealth Ombudsman (Ombudsman) under s 74 of the PID Act). Individuals and agencies must comply with those provisions. The guide also refers to the PID Rules, which the Minister may make under s 83 of the PID Act. However, no rules have been made at the time of publication of this guide.

The guide also includes suggestions for agencies to follow when applying the law: these are recommended as good practice but are not a legal requirement. Agencies may wish to adapt those suggestions to suit their own purposes, depending on their size, functions and contact with external entities. The Ombudsman and IGIS may follow their own procedures when investigating public interest disclosures.

If anything in this guide is inconsistent with requirements in the PID Act or the PID Standard as made and amended from time to time, the PID Act or Standard are to be followed. Unless otherwise indicated, references to legislative provisions in this Guide are references to sections of the PID Act.

2 How the public interest disclosure scheme works

- 2.1 The purpose of the PID Act
 - 2.2 What is a public interest disclosure?
 - 2.3 Who can make a public interest disclosure?
 - 2.4 Private interest vs public interest
 - 2.5 What can be disclosed?
 - 2.6 What is not disclosable conduct?
 - 2.7 Who can a public interest disclosure be made to?
 - 2.8 What happens if information is disclosed outside these circumstances?
-

2.1 THE PURPOSE OF THE PID ACT

The purpose of the PID Act is to promote the integrity and accountability of the Commonwealth public sector by:

- » encouraging and facilitating the making of disclosures of wrongdoing by public officials
- » ensuring that public officials who make protected disclosures are supported and protected from adverse consequences relating to the making of a disclosure
- » ensuring that disclosures are properly investigated and dealt with (ss 6, 7).

The PID Act complements existing notification, investigation and complaint handling schemes in the Commonwealth public sector. For example, where a public interest disclosure concerns suspected fraud, the investigation should be conducted in accordance with the Commonwealth Fraud Control Guidelines. The PID Act provides additional protections for disclosers and reporting obligations for agencies.

2.2 WHAT IS A PUBLIC INTEREST DISCLOSURE?

A public interest disclosure may be an internal disclosure, a legal practitioner disclosure, an external disclosure or an emergency disclosure, as set out in s 26(1). If a person makes a disclosure except in the circumstances defined in s 26(1), they are not protected from the consequences of breaching any privacy or confidentiality requirements that apply to the disclosed information.

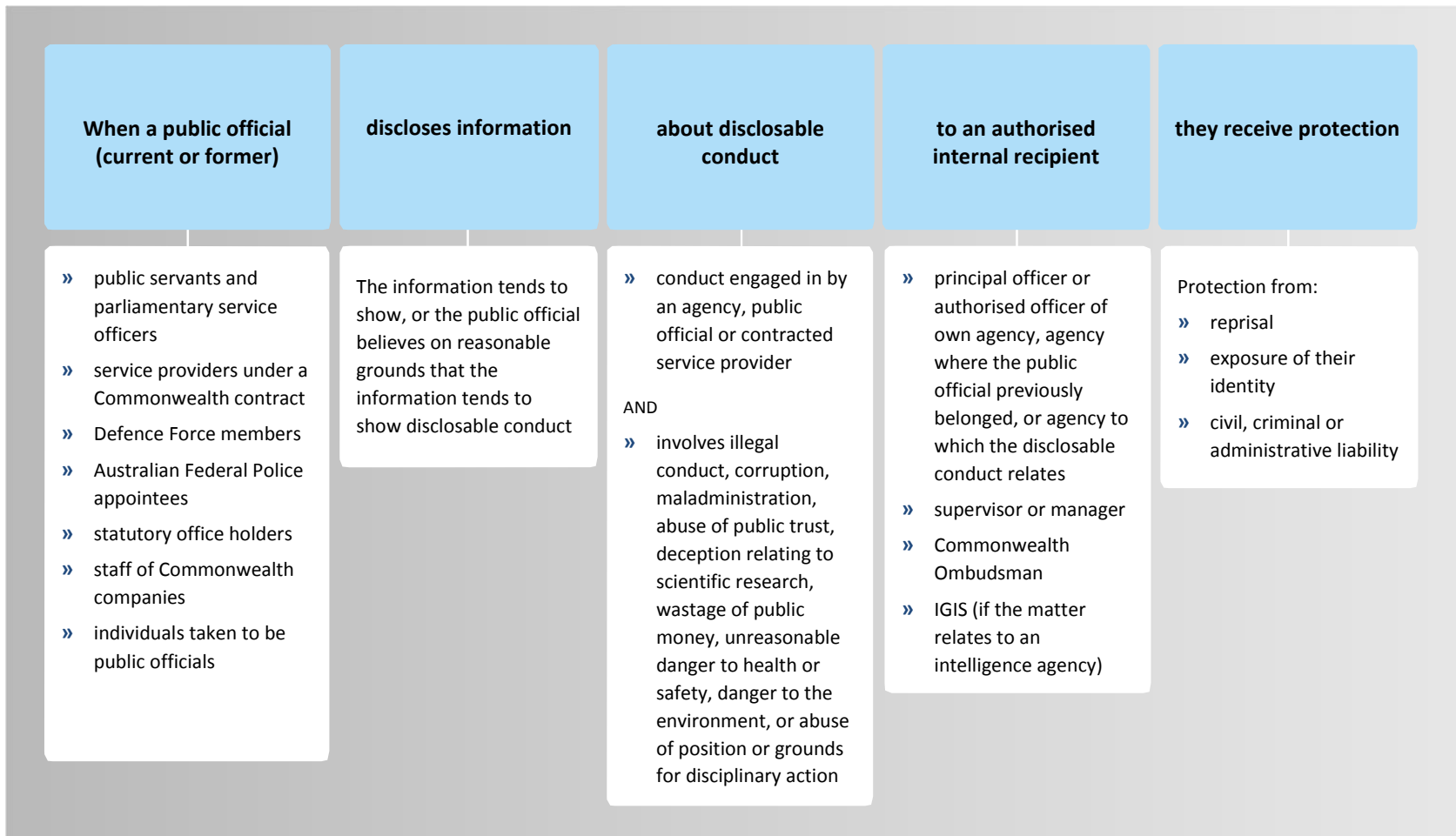
An internal disclosure is the most common type of disclosure under the PID Act. To make an internal public interest disclosure, the person disclosing suspected wrongdoing must:

1. be a current or former public official (or deemed to be a public official)
2. make their disclosure to the correct person within an Australian Government agency (their supervisor or an authorised internal recipient)
3. provide information that they believe tends to show, on reasonable grounds, disclosable conduct within an Australian Government agency or by a public official.

In limited circumstances a public official may disclose such information to a person outside government – this is known as an external disclosure or emergency disclosure. They can also make a disclosure to a legal practitioner for the purposes of getting advice about making one of the other forms of public interest disclosure.

The following diagram summarises the elements of making an internal disclosure under the PID Act.

Figure 1 – What is an internal public interest disclosure



2.3 WHO CAN MAKE A PUBLIC INTEREST DISCLOSURE?

2.3.1 Public officials

A person must be a current or former ‘public official’, as defined in s 69 of the PID Act, to make a public interest disclosure. In general, a person can make a disclosure if they belong, or previously belonged to, one of the agencies covered by the PID Act (see the list in 2.5.1.1 of this guide). This includes Commonwealth public servants, members of the Defence Force, appointees of the Australian Federal Police, Parliamentary Service employees, directors or staff of Commonwealth companies, statutory office holders or any other person who exercises powers under a Commonwealth law.

Individuals and organisations that provide goods or services under a Commonwealth contract (defined in s 30(3)) and their officers or employees are also public officials for the purposes of the PID Act. This includes subcontractors who are responsible for providing goods or services, either directly or indirectly, to an agency covered by the PID Act for the purposes of a Commonwealth contract (s 30(2)). See 2.5.1.3 for more information about Commonwealth contracts.

2.3.2 ‘Deemed’ public officials

An authorised officer may deem an individual to be a public official if they reasonably believe the individual has information about wrongdoing and proposes to make a disclosure (s 70). Authorised officers are the principal officer of an agency (i.e. the agency head) and officers that the principal officer appoints as authorised officers under the PID Act (s 36). It is not necessary for the disclosing individual to request that they be deemed a public official, but the authorised officer must provide the individual with a written notice of the determination.

An authorised officer might consider it appropriate to deem an individual to be a public official if the individual is not a public official, but nevertheless has ‘inside information’ about the agency’s wrongdoing. Examples might include:

- » a current or former volunteer with an agency
- » a member of an advisory body to a Commonwealth agency (where the members terms of engagement do not meet the definition of a public official)
- » an employee of an organisation that receives grant funding from the Australian Government, or
- » state and territory department officials who work alongside Commonwealth officials.

An authorised officer may also decide to deem a person to be a public official if they do not know, or cannot be certain whether the person is a public official, for example if the person is unwilling to provide identifying information for fear of reprisal. The relevant test is that the person was not a public official at the time the information they are disclosing was obtained (s 70(1)(b)). If the authorised officer is otherwise satisfied that the person is or has been a public official, then deeming is not required.

An authorised officer’s power to deem a person to be a public official operates only for the purposes of allowing that person to make a disclosure under the PID Act (s 70). An authorised officer cannot extend the reach of the PID Act by deeming a person to be a public official for the purposes of allowing a second person to make a disclosure about that first person’s conduct. Additionally, a judicial officer or member of a Royal Commission cannot be deemed a public official for the purposes of making a disclosure (s 70(3A)).

The formal requirements for an authorised officer to deem a person to be a public official are explained in 4.1.2 of this guide.

2.4 PRIVATE INTEREST VS PUBLIC INTEREST

The PID Act does not require an official to show that it is in the public interest for them to make a disclosure. A public official is therefore entitled to choose to make a disclosure under the PID Act about a matter that appears to reflect a personal interest, such as an individual grievance or workplace conflict, even if there is another mechanism available to them to report their concerns. If that disclosure meets the requirements in the PID Act, the fact that it is primarily a matter of personal interest is irrelevant. The agency's obligations under the PID Act to manage the disclosure will apply regardless.

When handling a PID about individual grievances or workplace conflict, it is appropriate for an agency to have regard to the overall seriousness of the subject matter of the disclosure, and the other mechanisms available to deal with it.¹ However, agencies should not assume that disclosures about conduct that appears to have only a private impact upon an individual are somehow less serious or do not warrant investigation under the PID Act. The individual's experience may be more broadly representative of a larger or systemic issue in that agency. For example a disclosure about bullying or harassment by the official's supervisor or colleagues may be representative of a more general culture of bullying or harassment in a particular work area.

2.5 WHAT CAN BE DISCLOSED?

Under s 26 of the PID Act, a public official can disclose information that they believe, on reasonable grounds, tends to show 'disclosable conduct'.

Disclosable conduct is defined in s 29 of the PID Act. There are two elements to the definition. The first element is that disclosable conduct has to be engaged in by a person or body covered by the PID Act (see 2.5.1 below). The second element is that the disclosable conduct has to be of a type covered by the PID Act (see 2.5.2 below).

2.5.1 Whose conduct?

Disclosable conduct covered by the PID Act has to be conduct on the part of one of the following:

- » an agency (see 2.5.1.1)
- » a public official in connection with their position (see 2.5.1.2)
- » an officer or employee of a contracted service provider, in connection with entering into or giving effect to a Commonwealth contract (see 2.5.1.3).

2.5.1.1 What is an 'agency'?

An agency is broadly defined (s 71). It means:

- » a Department
- » an Executive Agency under the *Public Service Act 1999* (Public Service Act) – that is, an agency established by the Governor-General rather than by legislation
- » a prescribed authority, described in s 72 as:
 - a statutory agency under the Public Service Act
 - a corporate Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*)
 - a Commonwealth company (see s 89 of the *Public Governance, Performance and Accountability Act 2013*)

¹ Chapter 6 explains when it may be appropriate to decide not to investigate a disclosure under the PID Act. Chapter 7 explains when it may be appropriate to conduct a different type of investigation under another Commonwealth law.

- the Australian Federal Police (AFP)
- one of the six intelligence agencies
 - the Australian Security Intelligence Organisation (ASIO)
 - the Australian Secret Intelligence Service (ASIS)
 - the Office of National Assessments (ONA)
 - the Australian Geospatial Intelligence Organisation (formerly known as the Defence Imagery and Geospatial Organisation)
 - the Defence Intelligence Organisation (DIO)
 - the Australian Signals Directorate (ASD, formerly known as the Defence Signals Directorate)
- the Australian Prudential Regulation Authority (APRA)
- the High Court, Federal Court and any other court created by parliament
- the Office of Official Secretary to the Governor-General
- the Commonwealth Ombudsman
- the Inspector-General of Intelligence and Security (IGIS)
- a body established by a Commonwealth law and prescribed by the PID rules²
- a person holding an office established by a Commonwealth law and prescribed by the PID rules³.

A Royal Commission is not a prescribed authority for the purposes of the PID Act.

2.5.1.2 *Who is a 'public official'?*

A 'public official' is defined in s 69 of the PID Act. It is a broad term which includes any person who belongs to one of the agencies covered by the PID Act (see 2.5.1.2). This covers Commonwealth public servants working in Departments, executive agencies and prescribed authorities, members of the Defence Force, appointees of the Australian Federal Police, Parliamentary Service employees, directors or staff members of a Commonwealth company, statutory office holders or any other person who exercises powers under a Commonwealth law.

Certain contracted service providers are also considered to be 'public officials' under the PID Act (s 30(2)). This includes:

- » individuals who are contracted service providers for a Commonwealth contract
- » individuals who are officers or employees of contracted service providers for a Commonwealth contract, and who provide services for the purposes of that contract
- » individuals who are subcontractors to a person who is a contracted service provider for a Commonwealth contract, and who provide services for the purposes of that Commonwealth contract.

2.5.1.3 *What is a contracted service provider for a Commonwealth contract?*

As noted in 2.5.1.2, the PID Act applies to contracted service providers for a 'Commonwealth contract'. A Commonwealth contract is defined in s 30(3) of the PID Act. It is a contract:

- » to which the Commonwealth, or a prescribed authority, is a party
- » under which goods or services are to be provided:
 - to the Commonwealth or a prescribed authority, or

² There are no PID rules at the time of publication.

³ See footnote 1.

- for or on behalf of the Commonwealth or a prescribed authority AND in connection with the Commonwealth's (or the prescribed authority's) performance of its functions or exercise of its powers.

Not all organisations who receive Commonwealth funding will automatically be covered by the PID Act. Contracts between the Commonwealth and another party under which goods or services are to be provided to the Commonwealth are covered by the PID Act and will be relatively straightforward to identify.

However, it is important to carefully examine the terms of any contract under which a party receives payment from the Commonwealth in return for providing goods and/or services to a non Commonwealth body or to individuals. As a general principle an organisation which is party to a contract that prescribes the terms for grant funding is not a contracted service provider for the purposes of the PID Act.

The fact that the PID Act may not apply to recipients of grant funding does not mean that agencies should not have systems in place to collect information that might be relevant to the conditions and administration of grants. Agencies should consider alternate ways of protecting and supporting individuals who may be important sources of information about how funded organisations are meeting their obligations.

2.5.2 What kinds of disclosable conduct are covered by the PID Act?

The kinds of conduct that a disclosure can be made about are listed in a table to s 29(1) of the PID Act. They are conduct that:

- » contravenes a Commonwealth, state or territory law
- » occurred in a foreign country and contravenes a foreign law that applies to the agency, official or service provider
- » perverts the course of justice
- » is corrupt
- » constitutes maladministration, including conduct that is based on improper motives or is unreasonable, unjust, oppressive or negligent
- » is an abuse of public trust
- » involves fabrication, falsification, plagiarism or deception relating to scientific research, or other misconduct in relation to scientific research, analysis or advice
- » results in wastage of public money or public property
- » unreasonably endangers health and safety
- » endangers the environment
- » is prescribed by the PID rules (s 29(1), however no PID rules have been made at the time of publication).

Disclosable conduct also includes conduct by a public official that:

- » involves or is engaged in for the purposes of abusing their position as a public official, or
- » could give reasonable grounds for disciplinary action against the public official (s 29(2)).

The term disciplinary action is not defined in the PID Act. It covers a range of actions taken by an employer intended to correct and/or punish an employee's wrongdoing (as opposed to underperformance). Disciplinary action does not include performance development and improvement activities for an employee, such as counselling, mediation or training.

Example:

APS employees must act in accordance with the APS Code of Conduct, which includes a requirement to uphold the APS Values and Employment principles. If an APS employee is found to have breached the Code of Conduct, an Agency Head may impose one or more sanctions listed in s 15(1) of the Public Service Act 1999. These sanctions include: termination of employment; reduction in classification; re-assignment of duties; reduction in salary; deductions from salary, by way of fine; or a reprimand. Conduct on the part of an APS employee that could, if proved; give reasonable grounds for a sanction under s 15(1) of the Public Service Act 1999 would meet the definition of 'disclosable conduct'.

2.5.3 Time limits for making a disclosure

There are no time limits for making a disclosure.

A disclosure can be made about conduct that occurred at any time, including before the PID Act commenced.

The PID Act continues to apply after:

- » the public official or contracted service provider alleged to have committed the wrongdoing has ceased to be a public official or contracted service provider (s 29(3)(a))
- » the agency ceases to exist (s 29(3)(b)).

However, if the age of the disclosed information would make an investigation impracticable, the principal officer or their delegate may decide not to investigate the disclosure (see 6.2.6.3 of this guide).

2.6 WHAT IS NOT DISCLOSABLE CONDUCT?

The PID Act has limited application to courts and tribunals. The following aspects of court and tribunal operations are excluded from the categories of disclosable conduct in the PID Act (s 32):

- » the conduct of judicial officers (defined in s 32(1))
- » the judicial functions of court staff, tribunal staff or tribunal members
- » any other conduct related to a court or tribunal unless it is of an administrative nature and does not relate to the management or hearing of matters before the court or tribunal.

The conduct of members of parliament is not covered by the PID Act (because they are not 'public officials' as defined in s 69). However, the departments of the Parliament and their employees are covered.

It is not disclosable conduct just because a person disagrees with:

- » a government policy or proposed policy
- » action or proposed action by a minister, the Speaker of the House of Representatives or the President of the Senate
- » expenditure or proposed expenditure related to such policy or action (s 31).

Disclosable conduct also does not include the proper performance of the functions and proper exercise of the powers of an intelligence agency or its officials (s 33).

Disclosable conduct by a public official must be conduct in connection with their position as a public official. In other words, conduct that is wholly private and has no bearing on their position as a public official is generally not disclosable conduct. However, serious unethical or criminal behaviour on the part of a public official, even if not connected to their employment, might nevertheless be grounds for

disciplinary action against the official, including termination of employment. Thus, conduct outside of the terms of employment that is nevertheless incompatible with the person's position as a public official would meet the extended definition of disclosable conduct in s 29(2)(b).

2.7 WHO CAN A PUBLIC INTEREST DISCLOSURE BE MADE TO?

A disclosure must be made⁴ to an appropriate person in order to gain the protections available under the PID Act (s 26). The PID Act focuses on the reporting and investigating of wrongdoing within government (internal disclosures), but allows for reporting outside government in specified circumstances (see 2.7.5 and 2.7.6).

2.7.1 Internal disclosure to the agency concerned

The majority of public interest disclosures made are internal disclosures made to the agency concerned. An internal disclosure attracts the protections of the PID Act for the discloser and brings into play obligations for the agency (and the official who received it).

Making a disclosure internally gives the agency the chance to investigate the matter and remove any danger or correct any wrong practices as quickly as possible. Each agency must have procedures for dealing with public interest disclosures (s 59), and should set out in its procedures how a disclosure should be made.

Under the PID Act, a public official can make an internal disclosure to their current supervisor (see 2.7.1.2) or an authorised officer (see 2.7.1.1) in:

- » their current agency or
- » the agency to which they previously belonged or
- » the agency to which the disclosure relates.

2.7.1.1 Who is an authorised officer for an agency?

Authorised officers for each agency are the principal officer (i.e. the agency head) and officers that the principal officer appoints as authorised officers under the PID Act (s 36). If a public official has information about suspected wrongdoing in an agency other than the one in which they work, they can choose to make their disclosure directly to an authorised officer in that other agency. If the agency has ceased to exist since the suspected wrongdoing took place, the appropriate agency is generally the agency that has taken over its functions (s 35(3)).

The PID Act extends to conduct on the part of individuals and entities that provide goods or services under a Commonwealth contract (see 2.5.1.3 for more information about what is considered to be a Commonwealth contract), concerning suspected wrongdoing related to entering into or giving effect to the contract. Disclosures about a contracted service provider's suspected wrongdoing can be made to an authorised officer appointed by the principal officer of the Commonwealth agency that is party to the contract (or directly to the principal officer).

2.7.1.2 Making an internal disclosure to a supervisor

A public official can also make a disclosure to their current supervisor (defined in s 8 to mean someone who supervises or manages them). A supervisor who receives a disclosure from someone they manage or supervise is obliged to give the information to an authorised officer in their agency as soon as reasonably practical (s 60A). The supervisor's obligation applies as soon as the supervisor has

⁴ The information may be disclosed in any form, and the discloser does not need to identify themselves, or that they are making a disclosure under the PID Act (or even intend to use it). See 4.1.4-5 of this guide for further explanation.

reasonable grounds to believe the information could concern one of more instances of disclosable conduct.

2.7.2 Internal disclosure to the Ombudsman or the IGIS

A public official can also make a disclosure to authorised officers of the Commonwealth Ombudsman, if they believe on reasonable grounds that it would be appropriate for the Ombudsman to investigate (ss 26(1), 34).

Authorised officers within the Ombudsman's office will seek information from the discloser about the reasons why they believe the Ombudsman should investigate their disclosure, rather than the agency to which the disclosure relates. In most cases, the Ombudsman will consider allocating the disclosure to the agency concerned for handling, unless that would be clearly inappropriate, for example, because of an unavoidable conflict of interest. If the disclosure concerns conduct that is action taken in relation to the employment of a person in the Australian Public Service or the service of a prescribed authority, the Ombudsman may not be authorised to investigate it (s 5(2)(d) of the *Ombudsman Act 1976*).

If the matter involves an intelligence agency or intelligence-related information, there are two options. The public official can make a disclosure to an authorised officer in the intelligence agency. Alternatively, if they believe on reasonable grounds that it would be appropriate for the IGIS to investigate, they may make a disclosure to an authorised officer of the IGIS (see www.igis.gov.au).

2.7.3 Internal disclosure to a prescribed investigative agency

The PID Act also allows for agencies with special investigative powers to be prescribed under PID rules. If the matter concerns their functions and powers, a disclosure may be made to those special investigative agencies. However, at the time of publication there are no prescribed investigative agencies.

2.7.4 Complaint to the Ombudsman or the IGIS

A public official can make a complaint to the Ombudsman if they believe the agency that received their internal disclosure did not appropriately deal with it (ss 5 and 5A *Ombudsman Act 1976*). If the disclosure relates to conduct of an intelligence agency, or an official belonging to an intelligence agency, the discloser may complain to the IGIS.

2.7.5 Disclosures to other people – emergency and external disclosures

A public official may wish to make a disclosure to other people, including people outside government (for example to the media, a union official or a member of parliament). They may also wish to publish the information more broadly, for example by using social media. However, this will rarely be permissible under the PID Act. The overall aim of the PID Act is to ensure that public officials disclose suspected wrongdoing to an authorised officer in an agency so that the agency can investigate and address the problem as soon as possible. Disclosures to people outside an agency, other than the Ombudsman, are protected by the PID Act only in the limited circumstances set out below.

Emergency and external disclosures cannot be made to a foreign public official and must not include any intelligence information. 'Intelligence information' is a term defined in s 41, and includes 'sensitive law enforcement information' which is also defined in s 41 (see 2.7.5.1)

The other specific restrictions that apply to emergency disclosures and external disclosure are complex, but a high level summary is provided below (see 2.7.6 and 2.7.7)

A public official contemplating making a disclosure to someone other than an authorised officer, their supervisor, the Ombudsman or the IGIS should consider seeking legal advice about the application of the PID Act to their circumstances. The Ombudsman's office can provide general guidance.

See 2.7.8 of this guide for an explanation of the protections for an official who makes a disclosure to a legal practitioner for the purposes of obtaining legal advice or assistance relevant to that official's proposed or actual disclosure.

2.7.5.1 Intelligence information and sensitive law enforcement information

'Intelligence information' is information, or a summary or extract of information, that:

- » has originated with or been received from an intelligence agency
- » might reveal such information or the technologies or operations of an intelligence agency
- » has been received from a foreign intelligence agency and might reveal a matter communicated in confidence
- » has originated or been received from the Department of Defence and might reveal operational intelligence or a program under which a foreign government provides restricted access to technology
- » identifies a current or former member or agent of ASIS or ASIO or could lead to their identity being reasonably inferred or established
- » is sensitive law enforcement information (see the full definition in s 41(1)).

'Sensitive law enforcement information' is information whose disclosure is reasonably likely to prejudice Australia's law enforcement interests, including a range of listed matters such as:

- » avoiding disruption to national and international law enforcement and criminal investigation
- » protecting informants and witnesses, and
- » protecting the technologies and methods used in dealing with criminal intelligence and investigation (see the full definition in s 41(2)).

2.7.5.2 Does an agency have to investigate an emergency or external disclosure?

The PID Act does not require a person who receives an emergency or external disclosure to take any action upon it, or pass it to the agency concerned. Nor is an agency required to take any particular action when it became aware of, or suspects that an emergency or external disclosure has been made. However, an agency is not precluded from investigating the subject matter, to ensure that appropriate action is or has been taken to address it.

2.7.6 Emergency disclosure

If a public official believes on reasonable grounds that the information they have concerns a substantial and imminent danger to the health or safety of one or more people or to the environment, they may make an emergency disclosure to any person except a foreign public official (s 26(1) item 3), provided they meet certain requirements:

- » The extent of the information they disclose must be only what is necessary to alert the recipient of the substantial and imminent danger.
- » If they have not previously made an internal disclosure about the matter, or if they have done so and the investigation is not yet completed, there must be exceptional circumstances justifying their decision to make an external disclosure. This might include, for example, if investigation was taking too long to complete having regard to the risk to a person's health and safety.

As noted above, an emergency disclosure must not include intelligence information or sensitive law enforcement information.

2.7.7 External disclosure

A public official who has already made an internal disclosure under the PID Act may subsequently make a disclosure to any person (except a foreign public official), if (s 26(1) item 2):

- » the final report of the internal PID investigation has not been prepared within 90 days of allocation, or the extended investigation period approved by the Ombudsman or IGIS (this condition does not apply to Ombudsman/IGIS investigations), or
- » the PID investigation has been completed and the discloser believes on reasonable grounds that the investigation was inadequate (see 2.7.7.1 of this guide), or
- » an investigation has been completed (whether the investigation was conducted under the PID Act or under other legislation) and the discloser believes on reasonable grounds that the response to the investigation was inadequate (see 2.7.7.1 of this guide).

As in the case of emergency disclosures, the external disclosure must not include intelligence information or sensitive law enforcement information (see 2.7.5.1).

Further, for an external disclosure, none of the information disclosed can concern the conduct of an intelligence agency. Also, the definition of 'disclosable conduct' excludes conduct that an intelligence agency or one of its officials, engages in as part of the proper exercise of the intelligence agency's functions (see 2.6 of this guide).

If the agency decides not to investigate the official's disclosure (i.e. by making a decision under s 48 of the PID Act), this would not meet the criteria for an official to make an external disclosure. The official may complain to the Ombudsman about the agency's decision not to investigate their disclosure. If the disclosure relates to one of the intelligence agencies, the official may complain to the IGIS.

Additional restrictions apply to external disclosures(s 26):

- » the public official must not disclose more information than is reasonably necessary to identify the wrongdoing
- » the externally disclosed information must have at least, in part, been the subject of a prior internal disclosure
- » on balance, making that external disclosure must not be contrary to the public interest (see 2.7.7.2 of this guide).

2.7.7.1 When is an investigation or subsequent action inadequate?

The PID Act does not define when an investigation or action taken by an agency as a result of the investigation is inadequate. However, an investigation is likely to be considered inadequate if:

- » the investigator showed bias or there was a strong apprehension of bias in how the investigation was conducted
- » information that was reasonably available, relevant and materially significant was not obtained
- » the findings or recommendations set out in the report were unreasonable on the basis of the information obtained during the investigation
- » the investigation report did not set out findings or recommendations that should reasonably have been made on the basis of the information obtained.

Some of the pitfalls for agencies to avoid when investigating a disclosure include:

- » significant delay in completing investigations

- » lack of awareness of legislation, procedures and guidance material
- » not maintaining confidentiality in investigations
- » conflicts of interest
- » giving witnesses the opportunity to collude
- » not pursuing obvious lines of enquiry
- » poor quality of investigation reports, with findings lacking sufficient substantiating evidence
- » investigators having little or no experience or training in conducting investigations.⁵

Action taken as a result of the investigation may be considered inadequate where the report recommended certain action be taken and no action was or is planned to be taken.

If the response to an investigation involves action that has been, is being or will be taken by a minister, the Speaker of the House of Representatives or the President of the Senate, that fact alone will not be grounds for a reasonable belief that the response is inadequate (s 26(2A)).

2.7.7.2 *What is 'contrary to the public interest'?*

The PID Act specifies various factors that must be taken into account in determining that a disclosure is not 'contrary to the public interest' for the purposes of making an external disclosure (s 26(3)). These are:

- » whether the disclosure would promote the integrity and accountability of the Commonwealth public sector
- » the extent to which the disclosure would expose a failure to address serious wrongdoing
- » the extent to which it would help to protect the person who made the disclosure from adverse consequences
- » the principle that disclosures should be properly investigated and dealt with
- » the nature and seriousness of the disclosable conduct
- » any risk that the disclosure could damage the security or defence of the Commonwealth, or its relations with a state or territory, Norfolk Island or another country
- » the principle that Cabinet information should remain confidential unless it is already lawfully publicly available
- » if any information was communicated in confidence by a foreign government or authority or an international organisation, the principle that such information should remain confidential unless consent is given
- » any risk that disclosure could prejudice the proper administration of justice
- » the principle that legal professional privilege should be maintained
- » any other relevant matter.

The identity and role or function of the person or body to whom the external disclosure is made is likely to be relevant when considering whether that disclosure is contrary to the public interest.

An official contemplating making an external disclosure may wish to consider first seeking legal advice (see 2.7.8) or a making a complaint to the Ombudsman's office or the IGIS (see 2.7.4).

⁵ See Ombudsman Victoria, Annual Report 2010, pp 74-76, for discussion of these recurring issues in public interest disclosure investigations in Victoria.

2.7.8 Disclosures to other people - legal practitioner disclosure

An official may make an emergency or external disclosure to a legal practitioner (as these disclosures may be made to any person other than a foreign public official in the circumstances discussed above).

There is also a specific category of public interest disclosure under the PID Act – ‘a legal practitioner disclosure’ - which allows a public official to disclose information to an Australian legal practitioner⁶ for the purposes of seeking legal advice or professional assistance in relation to the official’s actual or proposed disclosure elsewhere (i.e. an internal disclosure, an emergency disclosure or an external disclosure).

An Australian legal practitioner is an Australian lawyer admitted to the legal profession by a Supreme Court of an Australian State or Territory and who holds a practising certificate under a law of an Australian State or Territory (s 8 PID Act). In order to make a ‘legal practitioner disclosure’, the public official and lawyer in question need to be in a solicitor/client relationship.

For a ‘legal practitioner disclosure’, the official must not disclose intelligence information, including sensitive law enforcement information (s 26(1) item 4 - see 2.7.5.1 of this guide).

If the public official knew, or should reasonably have known, that any of the information they were disclosing had a national security or other protective security classification, the legal practitioner they make the disclosure to must hold an appropriate security clearance.

It is an offence for the legal practitioner to disclose to another person the information that the official (i.e. their client) disclosed to them, or to use that information for any purpose other than providing advice or assistance to the official relating to the official’s actual or proposed disclosure elsewhere (s 67).

2.8 WHAT HAPPENS IF INFORMATION IS DISCLOSED OUTSIDE THESE CIRCUMSTANCES?

Public officials are privy to a great deal of private and sensitive information about individuals and government matters. Maintaining strict confidentiality is an important part of a public official’s role and this obligation is often backed up by criminal sanctions.

A public official must use one of the proper avenues to gain the protections available under the PID Act. Those protections include confidentiality and immunity from criminal and civil liability or disciplinary action (see Chapter 8 of this guide).

A public official will not receive these protections if they give the information to someone outside government like a journalist, Member of Parliament or union representative, unless the conditions for an external or emergency disclosure are met. The official may be in breach of their duty to maintain appropriate confidentiality in relation to official information they have gained in the course of their work, or be subject to other civil, criminal or disciplinary action. For example, the official could be in breach of the *Crimes Act 1914*, s 79 (official secrets), or the secrecy/confidentiality provisions in the legislation under which the information was collected. If the disclosing official is an APS officer, they could be subject to disciplinary procedures under the APS Code of Conduct.

The limitations on protection under the PID Act should encourage public officials to make a disclosure to the people and agencies that have the responsibility to take action. Consistent with that aim, the PID Act requires agencies to have proper processes in place to manage an investigation and remedy problems, and mandates certain steps in handling an internal disclosure made in accordance with the provisions in the PID Act. These requirements are explored further in chapters 5, 6 and 7 of this guide.

⁶ An ‘Australian legal practitioner’

3 Agency obligations

3.1 Why public interest disclosures are important

3.2 Principal officer responsibilities

3.3 Other key PID roles and responsibilities

3.1 WHY PUBLIC INTEREST DISCLOSURES ARE IMPORTANT

The objects of the PID Act include encouraging and facilitating the making of public disclosures by public officials (s 6(b)). Making a public interest disclosure accords with the ethical culture of the Commonwealth public sector, including the employee's duty to act with integrity in the course of Australian Public Service and Parliamentary Service employment (s 13 of the *Public Service Act 1999*; s 13 *Parliamentary Service Act 1999*).

Employees and contractors have a close up perspective of what happens in the workplace. Those prepared to report wrongdoing may be important and reliable sources of information, identifying problems which should be addressed, including inefficient and unethical practices. However, many employees and contractors are reticent to report wrongdoing or to do so in a timely way. Disincentives to disclosing might include uncertainty over the seriousness of the problem, unwillingness to 'rock the boat', wishing to avoid conflict and protect career prospects, fear of reprisal and doubt that the agency will provide protection against it.

An effective public interest disclosure scheme has many benefits to agencies. Properly managed, the PID scheme enhances an agency's capacity to:

- » identify as early as possible conduct that needs correction
- » detect any weak or flawed systems which may make the agency vulnerable
- » deal with disclosed information appropriately and address problems before they escalate
- » avoid inefficiency and financial loss
- » reduce risks to the environment, or the health or safety of staff or the community
- » prevent damage to the agency's reputation and standing, and that of the Australian Government.

The PID Act, PID Standard and agency procedures can only go part way to creating an effective public interest disclosure scheme. An essential part of a successful scheme is the agency's commitment to encourage reporting of wrongdoing, acting on disclosures where appropriate and protecting disclosers from any adverse consequences.

Strong agency commitment to the public interest disclosure scheme requires:

- » policies and procedures that demonstrate the agency's endorsement of reporting suspected wrongdoing and the protection of disclosers
- » endorsement by senior management to the principles in the PID Act
- » commitment by supervisors and line managers, given that they will often be the first point of contact for disclosers and they have immediate responsibility for staff welfare
- » trust by public officials that agency procedures are sound and that the agency will ensure that disclosures will be acted on and disclosers will be protected from reprisal.⁷

⁷ P Roberts, A J Brown & J Olsen, *Whistling while they work*, 2011, ANU E Press, p. 18.

3.2 PRINCIPAL OFFICER RESPONSIBILITIES

The principal officer of each agency has a range of obligations under the PID Act aimed at ensuring that public officials who belong to that agency are aware they can make a disclosure; that the arrangements are publicised and accessible and that the agency deals appropriately with every disclosure made.

The principal officer is the agency head – that is, the departmental secretary, chief executive officer, Commissioner of the AFP, or other position as head of an agency, including an individual prescribed under the PID rules (see the full definition in s 73).

A principal officer's specific responsibilities under the PID Act include:

- » establishing internal procedures for facilitating and dealing with public interest disclosures relating to the agency (s 59(1)) - these procedures must include assessing risks that reprisals may be taken against a person who makes a disclosure, and providing for confidentiality of investigative processes)
- » taking reasonable steps to protect public officials who belong to the agency from detriment or threats of detriment (s 59(3)(a)) (discussed further in 8.5 of this guide)
- » appointing authorised officers (s 36)
- » ensuring there are sufficient authorised officers to be readily accessible to public officials who belong to the agency and that public officials are aware of their identity (ss 59(3)(b), (c))
- » notifying the discloser and the Ombudsman or IGIS as appropriate at various stages in handling a disclosure (ss 44, 50, 50A, 51(4))
- » ensuring disclosures are properly investigated (ss 47, 52, 53)
- » preparing an investigation report (s 51) and taking appropriate action in response to the report (s 59(4))
- » providing information and assistance to the Ombudsman and IGIS, including in relation to PID Act annual reporting (s 76(3)).

Each of these responsibilities is discussed in more detail in this guide. The principal officer can delegate any or all of those functions or powers to a public official who belongs to the agency (s 77(1)).

The principal officer is also an 'authorised officer' who can receive disclosures about his or her agency, or from the public officials who belong to the agency.

Most disclosures are likely to be made to the other authorised officers appointed by the principal officer (see 2.7.1.1 of this guide), or via a public official's supervisor (see 2.7.1.2). However, the principal officer remains an 'authorised officer' even after he or she appoints other authorised officers in the agency.

3.2.1 Appointing authorised officers and ensuring that officials can contact them

An authorised officer is a public official who belongs to the agency and is either the principal officer or is appointed in writing as such by the principal officer (s 36).

The principal officer must ensure that there is a sufficient number of authorised officers to be readily accessible to public officials who 'belong to' the agency (s 59(3)). This includes former public officials and staff of contracted service providers (s 69).

Authorised officers require good judgement and should be skilled in dealing with sensitive matters. They must be familiar with the provisions of the PID Act, so they can provide advice to disclosers and potential disclosers about the process and the protections available to them (s 60). Authorised officers do not necessarily have to be the most senior officers in an agency. Rather, it is important to establish a network of authorised officers who are approachable and accessible to all staff in the agency.

There is a risk that requiring disclosures to be made to a particular area or particular officer may discourage certain staff to be forthcoming or may raise a conflict of interest. In deciding how many authorised officers to appoint, and who they should be, the principal officer should consider such factors as:

- » the size of the agency
- » the profile and seniority of the officials who belong to the agency
- » the nature of the work performed in the agency
- » areas with higher risk and opportunity for 'disclosable conduct' such as fraud
- » the geographical location of staff (and their supervisors and managers).

The principal officer must ensure that public officials who belong to the agency are aware of the identity of each authorised officer in the agency (s 59(3)(c)). Section 5 of the PID standard says that principal officers must ensure that their agency provides an effective means for potential disclosers to find out how to contact authorised officers.

The contact details of authorised officers should be easy to find, for example, on the agency's intranet or in staff bulletins. Given that public interest disclosures may be made by former public officials or current public officials in other agencies, details for contacting authorised officers should be available on each agency's website.

Provided there are also avenues for making disclosures by telephone or in person, it is also open to an agency to set up an online system for receiving written disclosures, such as through a SmartForm, or to use a generic email address such as 'pid@agencyname.gov.au'. It is important, however, to restrict access to disclosures received through these 'indirect' channels, so that only people legitimately performing a function under the PID Act can become aware of the disclosed information (noting that only an authorised officer can receive and allocate an internal disclosure⁸).

3.2.2 Establishing agency PID procedures

The principal officer of each agency is responsible for establishing written procedures for effective management of public interest disclosures relating to their agency (s 59). Those procedures must conform to the PID Act and PID Standard. To minimise uncertainty within the agency, and to promote consistency in handling disclosures across the public sector, agency PID procedures should be comprehensive, clearly expressed and use terminology consistent with the PID Act and PID Standard.

Providing the legal requirements are met, agencies may develop their own policies and procedures to reflect their specific functions and responsibilities. Agencies may wish to specify in their PID procedures their preferred option for making a disclosure. For example, agencies may say in their procedures that it is preferable for officials to use other mechanisms to report and resolve grievances relating to their own employment, rather than using the PID Act. Alternatively, an agency's procedures might encourage officials to make disclosures about certain matters to an authorised officer in a particular area, or directly to an authorised officer rather than via a supervisor. However, an agency cannot prevent a person from making a disclosure via another avenue, such as via a manager or supervisor, or direct to the principal officer.

Each agency should carefully consider the target audience for its procedures. This includes current and former public officials, contracted service providers and their sub-contractors, as well as other people who might be 'deemed' public officials because they have information about suspected wrongdoing because of their close contact with agency officials (s 70 – see 2.3.2 of this guide).. The agency's PID procedures should not only be available to those people, but also be appropriate for their situation.

⁸ Although a supervisor may receive an internal disclosure from an official that he or she supervises, the supervisor's role in handling that disclosure is to pass the information to an authorised officer as soon as reasonably practicable (s 60A, PID Act).

Some agencies will choose to have an overarching policy document setting general principles, including the agency's commitment to public interest disclosures, expectations of staff and communication and training strategies; with a separate document containing more detailed procedures for receiving, managing and investigating public interest disclosures. Other agencies will prefer to include general policy and detailed procedures in the one document.

Whatever format is used, agency PID procedures should:

- » explain the legislative basis of the PID scheme and what it is about
- » state the agency's commitment to a culture that encourages reporting of inefficiency and wrongdoing
- » define 'public official' as that term applies within the specific agency
- » explain how someone may be 'deemed' a public official so they can make a disclosure
- » identify the types of wrongdoing that can be reported
- » set out the protections available under the PID Act, for disclosers and others (e.g. witnesses and officials suspected to be the discloser)
- » explain how reprisal risk will be assessed and when the risk assessment will be reviewed
- » outline confidentiality, anonymity and secrecy considerations at all stages of an agency handling a public interest disclosure
- » provide for thorough documentation of all actions, conversations and decisions (including the reasons) relating to a disclosure
- » include the contact details links for the agency's authorised officers, (or provide links to that information in a form accessible for all current and former officials belonging to the agency)
- » outline the investigative process and notification requirements
- » complement other relevant agency procedures, such as those relating to performance management, disciplinary action and investigation of fraud
- » specify how the agency will manage its reporting obligations to the Ombudsman and IGIS, as appropriate
- » include reference to the options of making a disclosure to the Ombudsman, IGIS or prescribed investigative agencies
- » set out the grounds under which external and emergency disclosures may be made.

3.2.3 Fostering agency culture

People are more likely to support the PID scheme and report wrongdoing if they trust that appropriate action will be taken and they will be supported for having raised their concerns and be protected from reprisals. In fostering a culture of disclosure, principal officers have a crucial role in ensuring that agency managers at all levels fully support reports of wrongdoing and are committed to ensuring appropriate action is taken.

Components of an agency culture which promotes disclosures include:

- » policies and procedures which demonstrate the agency's endorsement of the reporting of wrongdoing and the protection of disclosers, covering the officials who currently work in the agency, and also former staff and current and former contracted service providers
- » a clear statement of the agency's commitment to the highest standards of ethical and accountable conduct and support for officials who report wrongdoing. For greatest effect, this would be signed by the principal officer and placed at the start of the agency's policy or procedures on public interest disclosures.
- » adequate resources (both human and financial) allocated to implement the PID policies and procedures

- » senior managers who endorse the principles of the PID Act and work to ensure that managers below them have a positive attitude to the reporting of wrongdoing and are aware of their responsibilities under the PID Act
- » managers and supervisors who believe that early identification of concerns within their team or work unit will assist them to resolve issues directly and avoid criticism for having failed to prevent problems in the first place. Managers may themselves be disclosers.
- » line managers and supervisors who provide genuine support to disclosers and are empowered to effectively manage their workplace in the event of any conflict or threat of reprisal
- » specialist areas (such as human resources, internal audit and ethical standards units) that promote and advise people about the PID scheme and understand how it intersects with their work
- » proactive corporate governance systems which treat dealing with potential wrongdoing as part of the provision of a safer workplace, for example by taking reasonable steps to prevent and address inappropriate behaviour such as harassment and victimisation
- » staff who are aware of and support agency systems, policies and procedures relating to public interest disclosures.

3.2.4 Staff awareness and training

Each agency should ensure that its staff and contracted service providers are aware what a public interest disclosure is, what action to take if they suspect wrongdoing, how disclosures will be dealt with and the protections that are available to them. Research has shown a strong relationship between an employees' belief they are covered by public interest disclosure legislation and their likelihood of reporting wrongdoing.⁹

Staff training and awareness activities that focus on the PID Act can be a useful way to emphasise the positive aspects of a culture of disclosure. Agencies can explain that making a disclosure under the PID Act is one way for officials to report suspected wrongdoing. However, in some situations, less formal means of reporting will be sufficient and perhaps even preferable for simple matters. Agencies can emphasise the other reporting mechanisms available and give officials the information they need to choose the best path.

Agency PID procedures must be readily accessible to all current and former public officials belonging to an agency. At the very minimum, the procedures should be published on the agency's intranet page (for current employees) and on the agency's website for former employees and those who are providing goods or services to, or on behalf of, the agency under a Commonwealth contract. Publication of public interest disclosure procedures on the agency's website is consistent with the requirements of the Information Publication Scheme under the *Freedom of Information Act 1982* (FOI Act).

The Ombudsman's office has a range of information sheets and other guidance materials about PID on its website www.pid.ombudsman.gov.au. Agencies can download the Ombudsman's PID scheme logo to brand PID information on their internal and external websites. There are also downloadable promotional materials, including posters and that can be used as the basis for material targeted to the specific needs of each agency.

⁹ Roberts, Brown & Olsen p. 28, citing P Roberts, 'Evaluating agency responses: the comprehensiveness and impact of whistleblowing procedures' in A J Brown (ed) *Whistleblowing in the Australian public sector: enhancing the theory and practice of internal witness management in public sector organisations*, 2008, ANU E Press, Canberra, pp. 237-243.

3.2.4.1 Training

Agencies should consider the need to develop specialised training for different audiences amongst their staff:

- » Staff need general training about how to make a disclosure, their rights and obligations, the investigative process and outcomes. A guide for disclosers is available at www.pid.ombudsman.gov.au, and agencies should consider how this might be tailored for their own needs.
- » Managers and supervisors need to be trained to recognise when a matter may be a public interest disclosure and what action to take, including ensuring that staff are supported and protected against reprisals. They should be aware of how their agency's various policies (for example, on bullying and harassment, workplace health and safety, grievances and Code of Conduct matters) relate to each other, so that they can make judgements about the appropriate course of action. This type of training should be recognised as part of general management competency requirements.
- » Authorised officers need training about their specific responsibilities under the PID Act, including making allocation decisions, notification requirements, conducting risk assessments and supporting disclosers, and awareness of other avenues for staff to take action (such as bullying and harassment).
- » Investigators may need specialised training in conducting investigations, including investigation planning, procedural fairness requirements, interviewing witnesses, analysing evidence and report writing. It is up to each agency to ensure that the necessary specialist skills are available. However, it is appropriate for agencies to have a number of different investigators available with a variety of skills and experience, who can be allocated matters to investigate according to their skills and experience.
- » Staff in specialist areas (e.g. HR, Internal Audit, Fraud Prevention and Ethics/Dob-In Hotlines) need to understand how their subject matter interacts with the PID Act, and how an official may use the PID Act, and their agency's PID processes, to report suspected wrongdoing and gain protections for doing so.

3.3 OTHER KEY PID ROLES AND RESPONSIBILITIES

All public officials have responsibilities in relation to public interest disclosures. Some responsibilities are listed in the PID Act, while others reflect good corporate governance and ethical behaviour.

Following is a discussion of the role and responsibilities of:

- » authorised officers (see 3.3.1)
- » managers and supervisors (see 3.3.2)
- » other public officials (see 3.3.3).

3.3.1 Authorised officer responsibilities

Authorised officers are officers of an agency authorised in writing by the principal officer for the purposes of the PID Act (s 36). They 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 their agency (ss 26 and 34)
- » receiving disclosures from other public officials about conduct concerning their agency (ss 26 and 34)
- » deeming a person to be a public official to allow them to make a public interest disclosure (s 70)

- » explaining the requirements of the PID Act to disclosers
- » advising disclosers of any designated publication restrictions that apply to the information they have disclosed (s 60)¹⁰
- » assessing reported information to determine whether information could be considered to be a public interest disclosure (s 43(2))
- » making any preliminary inquiries necessary to make an allocation decision (s 43(4))
- » allocating all or part of the disclosure to the principal officer of their agency for handling and/or another agency that has agreed to handle the disclosure (ss 43(1) and (6))
- » notifying the principal officer of the agency of the allocation decision; the details of the disclosure and (if the discloser consents) the discloser's identity (s 44(1))
- » if any other agency has agreed to handle the disclosure, notifying the principal officer of that agency of the allocation decision; the details of the disclosure and (if the discloser consents) the discloser's identity (s 44(1))
- » notifying the Ombudsman (or IGIS where appropriate) of the allocation decision; the details of the disclosure and (if the discloser consents) the discloser's identity (s 44(1A)).
- » informing the discloser of the allocation decision (s 44(2))
- » consenting to the allocation of a disclosure by an authorised officer of another agency (s 43(6))
- » advising the discloser of a decision not to allocate, the reasons why and any other course of action that may be available under Commonwealth law (s 44(3)).

Agencies may also wish to designate a particular authorised officer, or an officer in another area to:

- » be a contact point in the agency for general advice about the operation of the PID Act
- » liaise with the Ombudsman or IGIS on related matters as required.

3.3.2 Manager and supervisor responsibilities

A public official may make a disclosure to their 'supervisor' (s 26). A supervisor includes any public official who supervises or manages the discloser (s 8). It is recommended that each agency's internal PID procedures clearly describe who is considered to be a supervisor or manager for which officials, by reference to the specific working arrangements and structure in that agency.

If the supervisor or manager believes that the information given to them concerns, or could concern, disclosable conduct, they must give that information to an authorised officer of the agency as soon as reasonably practicable (s 60A).

Managers and supervisors also have a key role in ensuring that the workplace culture supports the making of public interest disclosures. They can help to do so by:

- » having good general awareness of the PID Act and agency procedures, particularly in relation to what is 'disclosable conduct' and their obligation to inform an authorised officer
- » being careful to observe confidentiality requirements
- » knowing who the authorised officers are in their agency
- » being approachable to staff who wish to raise concerns
- » holding awareness sessions or discussion forums for their staff
- » ensuring staff undergo available training

¹⁰ A 'designated publication restriction' means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the *Family Law Act 1975* and the *Migration Act 1958*), witness protection and law enforcement mechanisms (see the full definition in s 8).

- » 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
- » paying close attention to interactions in the workplace where necessary (for example, if workplace conflict occurs after a disclosure is made or while it is being investigated)
- » ensuring identified problems in the workplace are corrected
- » setting an example for staff through their own conduct and ethical approach.

3.3.3 All staff responsibilities

Section 61 of the PID Act requires all public officials to use their 'best endeavours' to assist the principal officer in the conduct of an investigation, and to assist the Ombudsman or IGIS in their functions under the PID Act.

In an agency culture conducive to public interest disclosure, public officials might also be expected to share general responsibility for ensuring the system works effectively by:

- » 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
- » maintaining confidentiality whenever they are aware of the identity of a discloser, of anyone against whom an allegation has been made, or of anyone who has contributed to a disclosure investigation
- » supporting staff known to have made public interest disclosures
- » reporting to an appropriate person (a supervisor or authorised officer) any threats or reprisal action in relation to a disclosure.

4 Receiving internal disclosures

- 4.1 Receiving an internal disclosure from a public official
 - 4.2 What information should the discloser provide?
 - 4.3 Protection for the discloser
 - 4.4 The discloser's obligations
-

4.1 RECEIVING AN INTERNAL DISCLOSURE FROM A PUBLIC OFFICIAL

4.1.1 A current or former public official

As described in Chapter 2, a current or former public official may make a disclosure, and receive protection, under the PID Act. 'Public official' is broadly defined, covering people in or with a relevant connection to the Commonwealth public sector, including staff of contracted service providers (s 69). The agency's procedures should identify the categories of public officials that belong to that agency, taking into account all of the ways that it delivers its services to the public (including key contracted service providers and their officers or employees).

4.1.2 A 'deemed' public official

A person who is not a current or former public official can make a disclosure under the PID Act only if they are 'deemed' to be a public official by an authorised officer. As described in chapter 2, an authorised officer who believes on reasonable grounds that the person has information that concerns disclosable conduct (s 70) may 'deem' someone to be a public official so they can receive a disclosure from them about the agency to which the authorised officer belongs.

This may be appropriate, for example, if a former volunteer with an agency or someone who has received funding from the Australian Government has 'inside information' about the agency's wrongdoing. It might also be appropriate in circumstances where there is uncertainty around whether the person is a public official, and the authorised officer is satisfied that the person was not a public official at the time the information they are disclosing was obtained.

An authorised officer can deem a person to be a public official on the authorised officer's own initiative or in response to the person's request (s 70(2)). The authorised officer does this by issuing a written notice to the person stating that the PID Act has effect, and is taken always to have had effect, in relation to the disclosure of the information as if the individual had been a public official when they obtained the information (s 70(1)). This notice is not a legislative instrument (s 70(4)). If the authorised officer refuses a person's request that they be deemed a public official, the authorised officer must tell the person the reasons for their refusal (s 70(3)).

The power to deem a person to be a public official does not apply if the person is a judicial officer or a member of a Royal Commission (s 70(3A)).

4.1.3 Who can receive a public interest disclosure?

Agency procedures should make clear that a current or former public official has alternative ways to report suspected wrongdoing. Agencies may wish to specify in their procedures their preferred option for making a disclosure (for example, large agencies may have specialist integrity units). However, an

agency cannot prevent a person from making a disclosure via any of the relevant avenues specified in s 26 of the PID Act.

- » A current public official can disclose the information to someone who supervises or manages them. If the supervisor or manager believes that the information concerns, or could concern, one or more instances of disclosable conduct, the supervisor or manager must give the information to an authorised officer in the agency they belong to as soon as reasonably practicable (s 60A).¹¹
- » A current or former public official can disclose the information to an authorised officer of the agency they belong to (regardless of the agency the disclosure relates to).
- » If the disclosure relates to an agency other than the one the official belongs to (or if the person is a 'deemed' public official), the disclosure can be made to an authorised officer in the agency the disclosure relates to.
- » An authorised officer in the Ombudsman's Office or the Office of the IGIS or a prescribed investigative agency, if the discloser believes on reasonable grounds that one of these bodies is best placed to investigate their disclosure.¹² A public official may feel more comfortable making their disclosure to the Ombudsman, IGIS or an investigative agency if the disclosable conduct involves more senior staff in their agency or if they feel that reprisal is likely. However, the Ombudsman, IGIS or investigative agency may decide that it is appropriate to allocate the disclosure to the relevant agency for handling under the PID Act, depending on the subject matter and the circumstances of the discloser.

4.1.4 How can a public interest disclosure be made?

A person making a public interest disclosure does not need to expressly state, or even intend that the disclosure is made under the PID Act (s 28(3)). The person does not even have to know that the PID Act exists to make a disclosure or be covered by the protections in the Act. Simply conveying information about suspected wrongdoing to a person who is entitled to receive a disclosure under the PID Act (an authorised officer or supervisor) is sufficient.

The discloser's motive in making their disclosure is not relevant, as long as the information disclosed tends to show, on reasonable grounds, possible disclosable conduct. The person receiving the disclosure should focus on the substance of the information disclosed rather than speculate on why the disclosure is being made.

A person can make a public interest disclosure orally or in writing (s 28(1)). If a disclosure is made orally the officer receiving it (the authorised officer or supervisor) should make a record of what was said. It is good practice to ask the discloser to sign the record as being correct.

If a supervisor or manager is unsure whether the information disclosed to them tends to show disclosable conduct, they should err on the side of caution and refer the information to an authorised officer to determine whether it is a public interest disclosure. In all cases, the supervisor should let the official know that they intend referring the disclosed information to an authorised officer for assessment under the PID Act. If able to do so, the supervisor should explain to the official the protections given by the PID Act, or refer the person to an authorised officer who can do so.

4.1.5 Can a discloser be anonymous or use a pseudonym?

Disclosers do not have to identify themselves and may remain anonymous (s 28(2)). Remaining anonymous means disclosers do not identify themselves at any stage to anyone, including the authorised officer who receives the disclosure. If the disclosure comes from an email address from

¹¹ See 2.7.1.1 and 3.2.1 for an explanation of who is an authorised officer for an agency and how they are appointed.

¹² There are currently no prescribed investigative agencies.

which the person's identity cannot be determined, and the discloser does not identify themselves in the email, it should be treated as an anonymous disclosure.

Alternatively, a discloser may wish to use a pseudonym throughout the PID process. This may be appropriate in circumstances where the discloser is identifiable to their supervisor or an authorised officer, but decides to hide their identity to others. Consistent with the approach taken in the Australian Privacy Principles, and in addition to anonymity, pseudonymity should be made available as an option.¹³

One of the requirements for making a public interest disclosure is that the person is or was a public official (s 26(1)). This does not mean that the person has to prove their status beyond doubt. They may simply give information that supports that status, for example, by stating that they used to work for the agency or otherwise explaining how they know about the suspected wrongdoing they are reporting. If they do not, the authorised officer may wish to ask questions along these lines (if the person has provided contact details).

However, given the purpose of the PID Act is to encourage disclosure of suspected wrongdoing and ensure they are properly dealt with, authorised officers should be generous in their interpretation of the requirement that the discloser is a current or former public official, and treat an anonymous discloser as such unless the evidence on balance suggests otherwise. If the authorised officer is not satisfied that the discloser is or was a public official, they should consider whether to deem the person to be a public official (see 2.3.2 of this guide).

Agency procedures should state that disclosures may be made anonymously and clearly explain what anonymity entails, and when a person may wish to consider using a pseudonym instead. Staff should be assured that anonymous disclosures will be acted on whenever possible. However, the procedures should also note that there are reasons why staff might consider identifying themselves to an authorised officer, or at the very least providing a means of contact:

- » The PID Act requires agencies to keep a discloser's identity confidential, subject to limited exceptions including the discloser's consent (ss 20, 21). The person's identity may nonetheless become apparent if an investigation is commenced. If the person's identity needs to be disclosed or is likely to become apparent, the agency should discuss this with them.
- » It will be difficult to ensure protection from reprisal if the agency does not know the discloser's identity.
- » The authorised officer who receives an anonymous report must have reasonable grounds to suspect the disclosable conduct has occurred in order to allocate the matter for investigation. If they cannot contact the person to seek necessary further information, the matter may not proceed.
- » It may also be difficult to conduct an investigation if the discloser cannot be contacted for further information. An investigator has the discretion not to investigate, or investigate further, if the discloser does not provide their name and contact details or is unable to give the investigator further information or assistance if needed (s 48(1)(i)).
- » A discloser who does not provide a means of contact cannot be updated on the progress of the matter, including the outcome of the investigation.

Agency procedures should also note that a person who has made an anonymous disclosure may come forward at a later stage to disclose their identity and confirm that they have the protections of the PID Act.

¹³ See Australian Privacy Principle 2 published on the Office of the Australian Information Commissioner's website.

4.2 WHAT INFORMATION SHOULD THE DISCLOSER PROVIDE?

4.2.1 Information about the suspected wrongdoing

The PID Act does not require the discloser to prove that there has been disclosable conduct when they make a disclosure. The discloser only needs to provide sufficient information to tend to show one or more instances of disclosable conduct, or alternatively, that they honestly believe on reasonable grounds that there has been one or more instances of disclosable conduct. Once the disclosure is made, it is the agency's responsibility to decide whether and how to investigate it.

Agency procedures should:

- » advise disclosers to be clear and factual, and to avoid speculation, personal attacks and emotive language which can divert attention from the real issues in their disclosure
- » stipulate that disclosers should not investigate a matter themselves before making a disclosure as this may hinder a future investigation
- » inform disclosers that the sooner they raise their concerns, the easier it is likely to be for the agency to take action.

Agencies may wish to specify in their procedures that, depending on the circumstances, a discloser should think about covering as many of the following matters as possible in their disclosure so as to help the agency to determine how to proceed:

- » their name and contact details
- » the nature of the suspected wrongdoing
- » who they believed committed the suspected wrongdoing
- » when and where the suspected wrongdoing occurred
- » how they became aware of the suspected wrongdoing
- » whether the suspected wrongdoing has been reported to anyone else
- » if so, what has that person done to fix, stop or prevent it
- » whether they are concerned about possible reprisal as a result of making a disclosure.

Authorised officer should ask the discloser for any supporting correspondence or other documents, such as file notes or a diary of events, and the names of any people who witnessed the conduct or who may be able to verify what the discloser is saying.

4.2.2 Is the discloser's motive relevant?

A person receives protection if they report disclosable conduct in compliance with the PID Act. The discloser's motive or intention does not determine whether investigation is warranted. There can often be a history of conflict in a workplace, particularly if the person has tried to report wrongdoing in the past and they feel their concerns have been dismissed or ignored. This does not mean that their disclosure should be discounted. Authorised officers and supervisors receiving disclosures must be careful to look at the substance of the report rather than focusing on what they believe to be the person's motive for reporting.

When taking information from the discloser, it is nonetheless important to emphasise to the person that they should try to remain factual and focus on the issues related to the suspected wrongdoing rather than being emotive about individuals.

4.3 PROTECTION FOR THE DISCLOSER

A person who makes a disclosure about disclosable conduct in compliance with the PID Act will be covered by a range of legislated protections. These are discussed further in chapter 8 of this guide.

Even if the disclosed information turns out to be incorrect or unable to be substantiated, a discloser is protected by the PID Act, provided that they:

- » made their disclosure to an appropriate person under the PID Act and
- » honestly believed on reasonable grounds that the information tended to show disclosable conduct and
- » did not knowingly make false or misleading statements (s 11) and
- » did not knowingly provide information which contravenes a designated publication restriction¹⁴, without a reasonable excuse for that contravention (s 11A).

Agencies should make it clear that a person who makes a disclosure that is intentionally false or misleading will not gain the protections under the PID Act (s 11). Agencies may wish to refer an incident of false reporting to the appropriate area for consideration of disciplinary action. However, agencies should be cautious about referring borderline cases of false or misleading disclosure for disciplinary action, as this may unintentionally deter other staff from making disclosures.

Agency procedures should emphasise that making a disclosure does not automatically protect the discloser from the consequences of their own wrongdoing, including where they have been involved in the misconduct they are reporting. The discloser's immunity from liability under the PID Act relates only to the act of making the disclosure, not the conduct the disclosure is about.

Where a discloser comes forward with information that tends to show serious wrongdoing in which they had minor involvement, it is up to the agency to decide whether the discloser's actions should also be investigated and addressed.

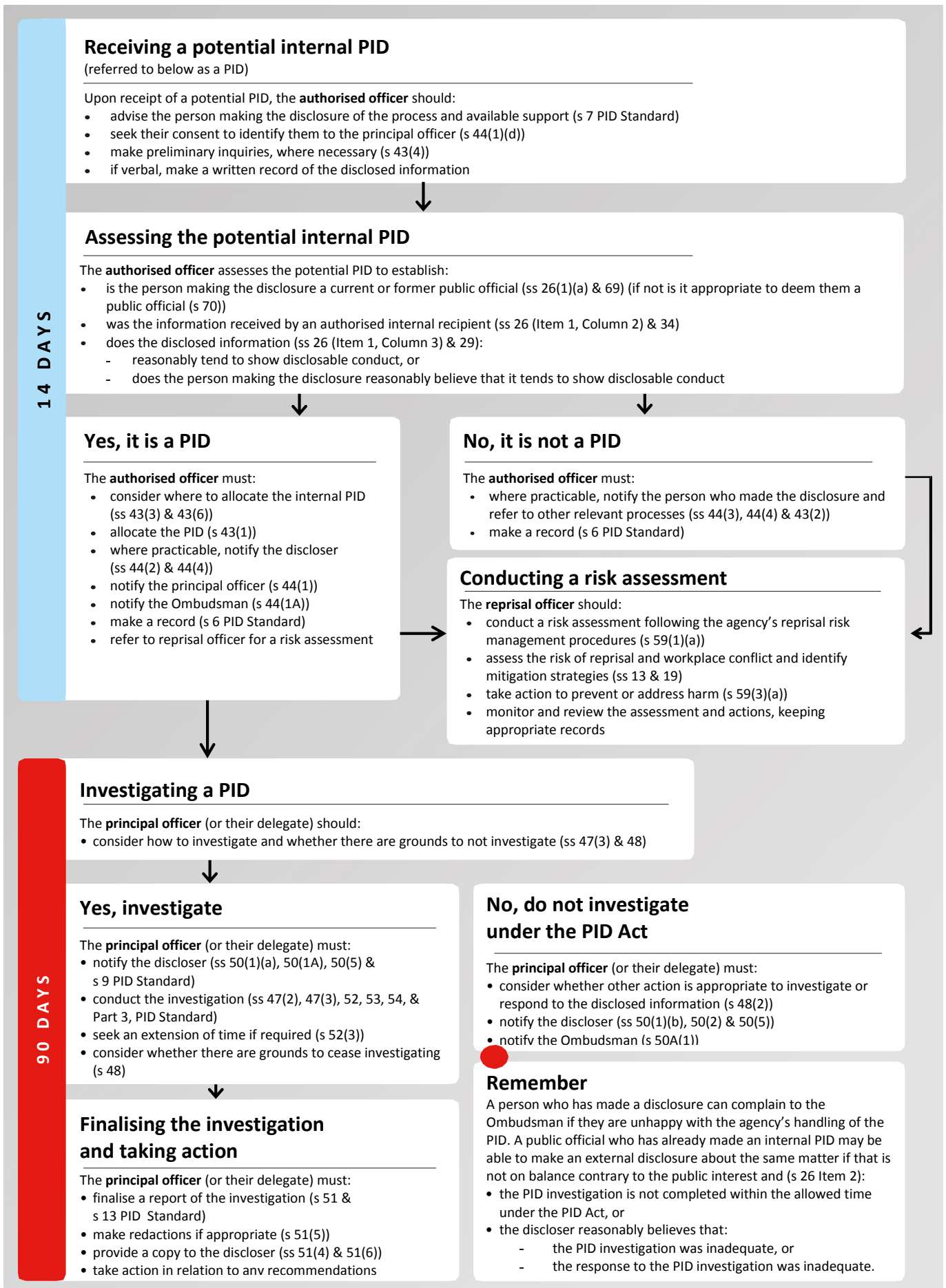
4.4 THE DISCLOSER'S OBLIGATIONS

The authorised officer should emphasise to the discloser that they should not discuss the details of their disclosure with anyone who does not need to know about it. Discussions with people who are not performing a function under the PID Act will not be for the purposes of the PID Act, and would therefore not be covered by the protections in the PID Act (unless the discussion meets the criteria for an External Disclosure, Emergency Disclosure or Legal Practitioner Disclosure, see 2.7.5 and 2.7.6 of this guide).

All public officials must use their best endeavours to assist in any investigation (s 61). The discloser should therefore be prepared to provide further information to help the investigator, as this will often be required.

¹⁴ A 'designated publication restriction' means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the *Family Law Act 1975* and the *Migration Act 1958*), witness protection and law enforcement mechanisms (see the full definition in s 8).

Figure 2 – Handling an internal disclosure under the PID Act



5 Initial assessment and allocation under the PID Act

- 5.1 Initial assessment of the disclosure
 - 5.2 Allocation under the PID Act
 - 5.3 Conducting an initial risk assessment
-

5.1 INITIAL ASSESSMENT OF THE DISCLOSURE

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

5.1.1 Determining if the information is an internal disclosure

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.

The initial assessment of a disclosure should be performed promptly. The authorised officer must allocate a disclosure (see 5.2 below) within 14 days of receiving it, unless there is a good reason why they need further time (s 43(5))

What constitutes an internal disclosure is set out at s 26(1). An internal disclosure is made when:

- » a person who is or has been a public official (see 4.1.1 and 4.1.2 of this guide)
- » discloses to an authorised internal recipient - or to their supervisor, who refers the information to an authorised internal recipient – (see 4.1.3 of this guide)
- » information which tends to show, or the discloser believes on reasonable grounds tends to show (discussed below in 5.1.2 of this guide)
- » one or more instances of disclosable conduct (see 2.5 and 2.6 of this guide).

5.1.2 Does the information tend to show disclosable conduct?

An internal disclosure under the PID Act must include information that:

- » tends to show disclosable conduct (an objective test) or
- » the discloser believes, on reasonable grounds, tends to show disclosable conduct (a subjective test).

To assist with the application of the subjective test, we discuss below the meaning of the terms 'belief on reasonable grounds' and 'tends to show disclosable conduct'.

5.1.2.1 *Belief on reasonable grounds*

A belief is more than a suspicion or assertion. To believe something, the person reporting the suspected wrongdoing must honestly hold the view that wrongdoing is more likely than not to have occurred. However, it is not sufficient for the discloser to personally hold the belief that wrongdoing has occurred: they must have 'reasonable grounds' for their belief.

Personal prejudice or animosity towards someone would not on its own be 'reasonable grounds' for a belief that wrongdoing has occurred. Some tangible support for the belief would be necessary. This could be based on direct observation of wrongdoing; evidence such as documentary records or missing

items of value; or corroboration by other people. It need not be evidence which would be admissible in a court of law (for example, hearsay could be considered).

The authorised officer will need to consider the disclosed information and decide whether it would lead a reasonable person to believe in the circumstances that wrongdoing is likely to have occurred. The discloser's motive for making the disclosure, or their personal opinion of the person(s) involved are unlikely to be relevant considerations.

5.1.2.2 *Tends to show*

A mere allegation with no supporting information is not sufficient to tend to show that wrongdoing has occurred or may be occurring: there must be sufficient information to support the allegation. If there is not, the discloser should be asked for additional information.

However, it is important to remember that a discloser does not need to prove their allegations. They only need to provide sufficient information to put the agency on notice that disclosable conduct may have occurred or be occurring.

Agencies should be careful not to encourage staff to investigate a matter themselves before making a disclosure; as such actions may prejudice a future investigation and may be beyond the staff member's authority.

If the authorised officer is not satisfied that there is a reasonable basis for considering the information to be an internal disclosure they are not required to allocate it to an agency for handling under the PID Act (s 43(2)). Some examples of matters which an authorised officer would not be satisfied are internal disclosures are:

- » a disclosure about the conduct of an employee of a state government agency
- » a disclosure that amounts only to an individual's disagreement with government policy
- » a disclosure that amounts only to a bare assertion that all officials within a particular team or branch are corrupt.

Section 43(5) of the PID Act requires the authorised officer to use their best endeavours to assess and allocate a disclosure within 14 days of receiving it, unless there is a good reason why they need further time. An example of an acceptable reason for taking more than 14 days to allocate a disclosure would be when it is necessary to undertake preliminary enquiries to decide whether a disclosure meets the threshold for an internal disclosure, but those inquiries cannot be concluded within 14 days.

If the authorised officer concludes that the disclosure does not meet the legislated requirement for an internal disclosure they must explain this to the discloser and explain any other options that they might have under Commonwealth law, for example, in relation to a workplace grievance (s 44(3)).

It is important to give the person as full an explanation as possible – for example, the person may have a genuine belief that the conduct they reported was improper, but they may not have been aware of surrounding circumstances which justify the conduct. Failing to give a proper explanation increases the likelihood that the person will lose trust in the agency's public interest disclosure process and may lead them to complain to the Ombudsman or IGIS.

If it is not reasonably practicable to contact the discloser, the authorised officer is not required to notify the discloser of their decision not to allocate the matter. However, the authorised officer should make a record of their decision and the reasons for it, and explain why contacting the discloser was not practicable. This record may be important if the Ombudsman or IGIS need to investigate the matter at a later date – for example, as a result of a complaint.

5.1.3 Preliminary inquiries

The PID Act gives an authorised officer the power to make any inquiries and obtain further information before making a decision about allocating the matter for handling under the PID Act (s 43(4)).

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 (refer to 4.1.3 Who can receive a public interest disclosure?)
- » who the disclosure should be allocated to for handling (provided that the answers to the two preceding questions is 'yes').

Preliminary inquiries could include asking the discloser for further details. The authorised officer should be careful to explain to the discloser why they are asking and avoid creating the perception that they doubt the discloser's truthfulness. The officer conducting preliminary inquiries should not seek evidence to confirm or contradict the discloser's information or to reach a conclusion about whether the alleged conduct occurred. This will be the task of the person to whom the PID is allocated for handling under the PID Act (discussed from 5.2 onwards).

An officer conducting preliminary inquiries should be careful not to express any criticism of the discloser or any person alleged to have committed a wrongdoing, as this can give rise to concerns of bias in a subsequent investigation. If there is evidence of criminal conduct at that early stage, and the matter is urgent (for example, if the information tends to suggest that a person is at imminent risk of physical harm) the authorised officer may consider referring that evidence to police in accordance with the agency's usual arrangements (s 53(3))¹⁵.

After making preliminary enquiries, if the authorised officer concludes that the disclosure does not meet the legislated requirement for an internal disclosure they should explain this to the discloser and explain any other options that they might have under Commonwealth law, for example, in relation to a workplace grievance (s 44(3)). As discussed at 5.1.2.2, providing as full an explanation of the decision as possible can help avoid a discloser losing trust in the agency's public interest disclosure process. Where the discloser is not reasonably contactable, the authorised officer should make a record of their decision and the reasons for it, and explain why contacting the discloser was not practicable.

5.2 ALLOCATION UNDER THE PID ACT

Once the authorised officer is satisfied that the disclosed information is an internal disclosure, they must allocate it for handling under the PID Act (s 43(1)).

5.2.1 Which agency should a disclosure be allocated to?

The authorised officer may allocate the handling of the disclosure to one or more agencies, including their own agency, the Ombudsman, the IGIS or a prescribed investigative agency¹⁶ (s 43).

In most cases, a disclosure should be allocated to the agency to which the disclosure relates. The principal officer for each agency is required to establish procedures for dealing with disclosures relating to that agency.

¹⁵ 7.3.6 of this guide explains the discretionary and mandatory provisions in the PID Act that apply to investigators who suspect that there is evidence of an offence, however, these do not limit the circumstances when others may decide to report a possible crime to the police.

¹⁶ There are currently no prescribed investigation agencies for the PID Act.

The agency that a disclosure relates to is will generally be apparent from the information the discloser provides. If it is not apparent, the authorised officer might wish to make preliminary inquiries to determine the most appropriate agency for allocation, including by discussing the issue further with the discloser or with an agency.

When considering which agency (or agencies) to allocate a disclosure to, the authorised officer must have regard to the principles in s 43(3):

- » an agency should not handle the disclosure unless some or all of the disclosable conduct relates to that agency
- » if the agency is the Ombudsman, some or all of the conduct relates to an agency other than an intelligence agency or the IGIS
- » if the agency is the IGIS, some or all of the conduct relates to an intelligence agency
- » if the agency is a prescribed investigative agency, that agency has the power to investigate the disclosure otherwise than under the PID Act (s 43(3)).

If the authorised officer wishes to allocate the disclosure to an agency other than their own, this may only be done with the consent of that other agency (see 5.2.3 below).

5.2.2 Allocation to more than one agency

While a disclosure can be allocated to more than one agency under s 43, the authorised officer should be careful that this does not create a situation where parallel investigations into the same matter occur. Allocation to more than one agency is unlikely to be appropriate except if a disclosure includes distinct issues that are best investigated by separate agencies. In circumstances where more than one agency is allocated a disclosure it is likely to be appropriate to inform each agency of the other's involvement.

5.2.3 Who needs to consent to the allocation?

If an authorised officer wishes to make an allocation to another agency, they must first obtain the consent of an authorised officer of that other agency (s 43(6)). It would normally be expected that if the matter relates to their agency's activities, the authorised officer would consent. If they do not consent, the authorised officer making the allocation decision will need to determine whether there is another appropriate agency or whether their own agency should investigate the matter.

The authorised officer making the allocation decision may find it appropriate to contact the other agency early in the decision making process, particularly if they would like some preliminary information to assist them in determining if the matter should be allocated to the other agency.

Agencies that have many authorised officers should consider nominating one officer to coordinate and consent to allocations from other agencies so as to streamline their processes.

5.2.4 Can subsequent allocations be made?

An authorised officer may, after allocating a disclosure to one or more agencies, decide later to allocate part or all of the disclosure to another agency (s 45). This may happen if the true nature or extent of a problem only becomes apparent during an investigation (for example, if the investigation reveals that staff in another agency appear to have been involved in wrongdoing).

5.2.5 Giving notice of the allocation

Once the authorised officer decides to allocate a disclosure to an agency, they must inform:

- » the principal officer of the agency to which the disclosure is allocated (s 44(1))

- » the Ombudsman (or the IGIS, if allocated to one of the intelligence agencies) (s 44(1A))
- » the discloser (s 44(2)).

5.2.5.1 *Informing the principal officer of the allocation*

When the authorised officer decides to allocate a disclosure to an agency for handling under the PID Act they must inform the principal officer of that agency (s 44(1)):

- » that the disclosure has been allocated to their agency
- » the information that was disclosed
- » the suspected disclosable conduct
- » the discloser's name and contact details, if known to the authorised officer (but only if the discloser consents – s 44(1)(d)).

The authorised officer should ensure that they ask the discloser for their consent to pass their contact details to the receiving agency. If the discloser declines, the authorised officer should advise the receiving agency that the discloser was asked and did not consent. If the discloser does not consent to their identity being revealed, they could be asked if they would like to provide an anonymous means of contact (such as an email address that does not include their name), so that they can at least be notified of the progress of the matter as required by the PID Act. The information that is allocated for investigation may need to be redacted to avoid the discloser being identified, and the discloser should be advised this may affect the ability of the agency to investigate their public interest disclosure.

If the authorised officer allocates the disclosure to more than one agency, they must provide this information to the principal officer of each agency.

5.2.5.2 *Informing the Ombudsman or IGIS of the allocation*

When an authorised officer allocates a disclosure to any agency for handling under the PID Act, they must also inform the Ombudsman (or IGIS, if the disclosure is allocated to an intelligence agency) of the same matters they are obliged to inform the principal officer of the receiving agency (s 44(1A)). The discloser's name and contact details should not be provided to the oversight agency unless the discloser consents.

While the full details of the information disclosed should be provided to the principal officer of the agency, a brief outline or synopsis is sufficient for the Ombudsman or the IGIS. This will assist in managing security concerns and protecting the confidentiality of the matter.

Authorised officers in those agencies required to report to the Ombudsman may use the form published on the Ombudsman's website to notify when they have allocated a disclosure.¹⁷ The IGIS does not have a required format for notifications from the intelligence agencies.

5.2.5.3 *Informing the discloser of the allocation decision*

The authorised officer must inform the discloser that they have allocated their disclosure for handling under the PID Act (s 44(2)). This should be done as soon as practicable.

It is not compulsory for the discloser to be informed of the allocation decision in writing. However, the authorised officer should make a written record of their decision and when and how they notified the discloser (see 5.2.6 below).

If the authorised officer has decided to allocate the disclosure to their own agency for handling, they should also inform the discloser about the principal officer's powers to decide not to investigate the disclosure, or stop investigating it (see 6.1.1 of this guide, and s 9, PID Standard).

¹⁷ Forms to notify the Ombudsman are available on the Ombudsman's website at www.PID.ombudman.gov.au.

The discloser may be notified of the allocation and investigation decisions in the one document (s 50(4)). However, this should only be done if the two decisions are close in time. The notice requirements for a decision not to investigate a disclosure are explained in 6.5.1 of this guide. The notice requirements when the disclosure is to be investigated are explained in 7.1.1 of this guide.

If it is not reasonably practicable to contact the discloser, the authorised officer is not required to notify the discloser of their allocation decision (s 44(4)). However, the authorised officer must still make a record of the decision and the reasons for it (see 5.2.6.1 of this guide).

5.2.6 What records must the authorised officer make of their allocation?

The authorised officer should make a written record of their allocation decision, the reasons for the decision and the receiving agency's consent to the allocation (if allocated to another agency for handling). Section 6(1) of the PID Standard provides that this requirement must be included in each agency's PID procedures.

The authorised officer should also make a written record of whether the discloser was notified of the allocation decision and the details of how that happened. Section 6(2) of the PID Standard provides that each agency's PID procedures must require appropriate records of the date, time and means of notification, and the content of the notification to the discloser.

The authorised officer should also make a written record of their risk assessment and any action taken to protect or support the discloser (see 5.3 of this guide).

5.2.6.1 What if the authorised officer cannot contact the discloser?

The authorised officer need not notify the discloser of their allocation decision if it is not reasonably practicable to do so (s 44(4)). If the authorised officer considers it is not reasonably practicable to contact the discloser, they should make a record explaining why, including details of the time, date and method of any contact attempts made.


5.3 CONDUCTING AN INITIAL RISK ASSESSMENT

Agency procedures must include arrangements for assessing the risks that reprisals may be taken against a person who makes a public interest disclosure (s 59(1)(a)). This involves assessing the specific behaviour and circumstances that may result in reprisals, and then putting in place appropriate strategies to prevent or contain them. Detailed information about risk assessments is included at 8.5 of this guide onwards.

5.3.1 Protection of the discloser's identity

One aspect of the risk assessment is assessing the likelihood of the discloser's identity becoming known. Disclosers will often be anxious about the prospect of their identity being revealed. The authorised officer should assure the discloser that their identity will be protected as much as possible at all times and of the procedures that are in place to ensure confidentiality of the investigation process. The specific legal protections in the PID Act for the discloser's identity are discussed in 8.2 of this guide.

However, it is important that authorised officers give a discloser honest and realistic expectations about the agency's capacity to prevent their identity as the source of the disclosed information becoming known. The discloser must be made aware that, to investigate a matter, their identity will quite possibly become apparent. For example, if the discloser is one of a very small number of people who have access to the relevant information, or if the information they have disclosed was something they were told privately and in confidence, others may guess they were the source of the information.



However, the agency has an obligation to take reasonable steps to support and protect them from detriment as result of making a disclosure. The PID Act also makes it an offence for anyone to take or threaten reprisal against a discloser and provides access to a court for remedies. Chapter 8 of this guide contains detailed information about the legal protections in the PID Act for disclosers and others.

6 Deciding whether to investigate under the PID Act

- 6.1 General requirement to investigate a disclosure
 - 6.2 When can an agency decide not to investigate?
 - 6.3 Does a decision not to investigate prevent other action?
 - 6.4 What records must be made of a decision not to investigate?
 - 6.5 Who must be notified of a decision not to investigate?
-

6.1 GENERAL REQUIREMENT TO INVESTIGATE A DISCLOSURE

Once a disclosure had been allocated to an agency for handling under the PID Act, the principal officer of that agency is obliged to investigate it (s 47).

However, the principal officer may decide not to investigate the disclosure, or to stop investigating it, if one of the discretionary grounds in s 48 of the PID Act apply. This chapter explains when it may be appropriate for the principal officer to decide not to investigate a disclosure under the PID Act.

The principal officer may delegate any of their functions or powers to a public official who belongs to the agency (s 77). References to the principal officer in this chapter include references to their delegates, including an investigator.

6.1.1 Advising the discloser about the principal officer's powers

Section 9 of the PID Standard requires an agency allocated a disclosure for handling under the PID Act to inform the discloser about the principal officer's powers to decide:

- » not to investigate the disclosure under the PID Act, or to stop a PID investigation that has started (discussed in this chapter) or
- » to investigate the disclosure under a separate investigative power (discussed in 7.2.1 of this guide).

The discloser must be given that information within 14 days after the disclosure is allocated to the agency for handling under the PID Act, if it is reasonably practicable to do so.

In practice, where the authorised officer has allocated the disclosure within his or her agency for handling, this information can be given to the discloser at the same time as the notice of allocation (see 5.2.5.3 of this guide). Where the disclosure is allocated to a different agency for handling, the receiving agency must provide this information to the discloser.

6.2 WHEN CAN AN AGENCY DECIDE NOT TO INVESTIGATE?

The principal officer may decide not to investigate a disclosure under the PID Act only on a ground set out in s 48, that is, if:

- » the discloser is not a current or former public official (see 6.2.1)
- » the information does not, to any extent, concern serious disclosable conduct (see 6.2.2)
- » the disclosure is frivolous or vexatious (see 6.2.3)
- » the disclosure is the same or substantially the same as another disclosure which has been or is being investigated under the PID Act (see 6.2.4.1)

- » 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 (see 6.2.4.2)
- » 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 is reasonably satisfied that there are no matters that warrant further investigation (see 6.2.4.2)
- » the discloser has advised the principal officer that they do not wish the investigation to be pursued, and the principal officer is reasonably satisfied that there are no matters that warrant further investigation (see 6.2.5)
- » it is impracticable to investigate the disclosure because (see 6.2.6):
 - 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 investigator the information or assistance they requested.

If the investigation has already started, the principal officer may subsequently decide to stop the investigation on one of the discretionary grounds set out above.

6.2.1 The discloser is not a public official

In order to make a public interest disclosure, a person must be a public official, or a deemed public official (see 2.3 of this guide). If an authorised officer has allocated a disclosure in the mistaken belief that the discloser is a public official, the principal officer or their delegate may decide not to conduct an investigation, or stop an investigation that has already started (s 48(1)(a)).

The principal officer or their delegate may consider it is appropriate to continue the investigation, given the nature of the disclosed information, despite the fact that the discloser has never been a public official. If so, the authorised officer who allocated the disclosure should be asked to consider whether it is appropriate to deem the discloser to be a public official (see 2.3.2 and 4.1.2 of this guide).¹⁸ A determination to deem the person a public official would place the investigation on a proper footing, and entitle the discloser to protection under the PID Act.

6.2.2 The disclosed information does not concern serious disclosable conduct

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if the disclosed information does not, to any extent, concern serious disclosable conduct (s 48(1)(c)). This means that in some situations, information about conduct that meets the threshold of disclosable conduct will not be considered serious enough to warrant an investigation under the PID Act.

6.2.2.1 What is serious disclosable conduct?

The term ‘disclosable conduct’ is defined in s 29 of the PID Act and discussed in 2.5.2 of this guide. However, the PID Act does not define ‘serious disclosable conduct’. It is a matter for the principal officer or their delegate to decide whether the alleged conduct is serious. The principal officer should consider all the relevant circumstances based on the information before them. Factors which might be considered could include:

- » whether the wrongdoing, if proven, involves an offence with a significant penalty or would lead to disciplinary action or other similar consequences

¹⁸ Alternatively, if the investigation officer is also an authorised officer, he or she may consider whether to make a determination under s 70 of the PID Act (see 2.3.2 of this guide).

- » whether the wrongdoing was one of a series of incidents that indicates a course of conduct
- » the level of trust, confidence or responsibility placed in a public official who is alleged to have acted wrongly
- » the level of risk to others or to the Commonwealth
- » the harm or potential harm arising from the conduct, including the amount of public money wasted
- » the benefit or potential benefit derived by the public official or others
- » whether the public official acted in concert with others, and the nature of their involvement
- » any apparent premeditation or consciousness of wrongdoing
- » what the public official ought to have done and how their conduct might reasonably be viewed by their professional peers
- » any applicable codes of conduct or policies
- » maladministration that relates to significant failure in the administration of government policy, programs or procedures.

This list is not exhaustive and is provided as a guide to the types of issues that might be considered when determining if disclosable conduct is serious. If an agency's PID procedures include guidance about when a matter might be considered 'serious' they should not be written in such a way that they could be seen to fetter a delegate's discretion.

It is important to remember that s 48(1)(c) is a discretionary ground. If the principal officer forms the view that the disclosure does not concern serious disclosable conduct, but considers it should still be investigated, they may continue the PID investigation. (See also 6.3 below.)

6.2.3 What is meant by frivolous or vexatious?

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if the disclosure is frivolous or vexatious (s 48(1)(d)).

An example of a frivolous disclosure would be something so minor that no action is warranted, for example, a complaint that a public official made a minor error in a written document without any resulting disadvantage to anyone. In such a situation, it would also be acceptable for the principal officer or their delegate to decide not to investigate on the basis that the information does not to any extent concern serious disclosable conduct (see 6.2.2).

In determining whether a disclosure is vexatious, the principal officer should consider such factors as whether:

- » the disclosure was made with the sole intention of annoying or embarrassing someone, or was made for another purpose, rather than being made in good faith by a person concerned about stopping or preventing wrongdoing
- » the allegations are so obviously untenable or manifestly groundless that they cannot possibly be made out.¹⁹

However, the principal officer should be careful not to dismiss a disclosure merely because it appears to arise from workplace conflict or be associated with animosity, since it may also involve substantive issues of misconduct or wrongdoing which should be investigated.

¹⁹ *Attorney General v Wentworth* (1988) 14 NSWLR 481, 491.

6.2.4 Prior or current investigation of same matter

The PID Act contains several discretionary grounds that allow a principal officer or their delegate to decide not to investigate a disclosure if the information concerns conduct that has already been investigated, or is currently under investigation. If a PID investigation has already commenced, the principal officer may decide to stop the investigation on these same grounds. The requirements are discussed in 6.2.4.1 and 6.2.4.2 below.

6.2.4.1 Investigated under the PID Act

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if the disclosed information is the same or substantially the same as information about conduct that has already been investigated under the PID Act, or is currently being investigated under the PID Act (s 48(1)(e)). The other PID investigation could be in response to a disclosure made by a different public official.

It may also be appropriate to use this ground to decide not to investigate a second or subsequent disclosure made by the same public official who is dissatisfied with the outcome the investigation of their earlier disclosure. In such a case, the principal officer should carefully consider whether the official has provided any additional information to suggest that further investigation of the matter is warranted.

6.2.4.2 Investigated under another law of the Commonwealth or the Commonwealth's Executive power

Current investigation: The principal officer or their delegate may decide not to investigate a disclosure under the PID Act if it concerns conduct that is currently being investigated under a different Commonwealth law (or procedures established under a Commonwealth law other than the PID Act – s 48(3)), or the Commonwealth's executive power, and it would be inappropriate to conduct a PID investigation at the same time (s 48(1)(f)).

The conduct already under investigation must be the same or substantially the same as the conduct the disclosure was about. If a PID investigation has already commenced, the principal officer may decide to stop the PID investigation on these same grounds.

Prior investigation: The principal officer or their delegate may decide not to investigate a disclosure under the PID Act if it concerns conduct that has already been investigated under a different Commonwealth law, or the Commonwealth's executive power. The principal officer or their delegate must be reasonably satisfied that there are no further matters in the disclosure that warrant investigation (s 48(1)(g)). The conduct previously investigated must be the same or substantially the same as the conduct the disclosure was about.

The prior or current investigation does not need to be in response to information provided by the official who made the disclosure. In most cases, the conduct will have been identified through other means. It is important to note that it is the conduct that must be the same as that subject to the other investigation, not the discloser or circumstances of the conduct coming to light through other processes.

6.2.4.3 What sorts of investigations can be conducted under other Commonwealth laws?

Listed below are some other types of investigations (and the relevant Commonwealth laws) that could provide a basis for a principal officer to exercise their discretion under s 48(1)(f) or (g) of the PID Act.²⁰

²⁰ At the conclusion of a PID investigation, it may be appropriate to refer a matter for further investigation under one of these laws. 7.3.4 of this guide explains how this is different from making a decision to not investigate a disclosure, or to stop investigating a disclosure under s 48 (1)(f) or (g) of the PID Act.

- » a Code of Conduct investigation under the *Public Service Act 1999*
- » a Code of Conduct investigation under the *Parliamentary Service Act 1999*
- » an investigation under the *Fair Work Act 2009*
- » an investigation under the *Work Health and Safety Act 2011*
- » a Professional Standards investigation under the *Australian Federal Police Act 1979*
- » a Code of Conduct investigation, or disciplinary or Redress of Grievance process under Defence Force legislation or regulations
- » a fraud investigation under s 10 of the *Public Governance, Performance and Accountability Rule 2014*
- » an investigation under the *Ombudsman Act 1976*
- » an investigation under the *Inspector-General of Intelligence and Security Act 1986*.

6.2.5 The discloser does not want an investigation

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if the discloser has advised the principal officer that they do not wish the investigation to be pursued, **and** the principal officer is reasonably satisfied that there are no matters that warrant further investigation (s 48(1)(h)).

One situation where this ground might apply is if an official unintentionally makes a disclosure. As explained in 4.1.4 of this guide, a public official conveying information about suspected wrongdoing to a person who is entitled to receive a disclosure under the PID Act (an authorised officer or supervisor) is all that is required to make an internal disclosure.

For example, an official might tell their supervisor something, or say something to a person who is an authorised officer, without realising that the information concerns disclosable conduct and that their disclosure will trigger obligations and protections under the PID Act. Once the criteria for an internal disclosure are met, the authorised officer is obliged to allocate the disclosure for handling under the PID Act and advise the discloser accordingly. At this point, the official might ask to withdraw their disclosure.

A person who has made a disclosure cannot simply withdraw it and they do not have to consent to an investigation. If a public official asks to withdraw their disclosure, the principal officer or their delegate should seek to understand the reasons for that request. It would clearly be inappropriate not to investigate a disclosure if the official who made it was reluctant to cooperate in case their own wrongdoing came to light. On the other hand, if the discloser is concerned about their identity becoming known, or reprisal action being taken, it would be appropriate to put in place measures to mitigate those risks (or provide reassurance if this has already been done). Depending upon the subject matter of the disclosure, and whether action is already in train to address it, the principal officer might consider that there are no matters that warrant further investigation.

6.2.6 Investigation of the disclosure is impracticable

There are three separate grounds upon which a decision can be made to not investigate a disclosure because it would be impracticable. They are discussed in 6.2.6.1 to 6.2.6.3 of this guide.

6.2.6.1 Discloser's name and contact details unknown

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if an investigation is impracticable because the discloser has not disclosed their name and contact details (s 48(1)(i)).

This ground might apply when a disclosure is made anonymously and the discloser has also refused or omitted to provide the authorised officer with any means of contacting them. It might also apply if the discloser has provided the authorised officer with his or her name and contact details, but has not consented to that information being provided to the principal officer. However, the principal officer or their delegate must also consider whether in the absence of that information it would be impracticable to investigate the disclosure.

The PID Act specifically permits disclosures to be made anonymously or using a pseudonym (see 4.1.5 of this guide), and for a discloser to refuse to be identified to the principal officer (see 5.2.5.1 of this guide). The objects of the PID Act include ensuring that disclosures by public officials are properly investigated and dealt with (s 6(d)). Accordingly, before making a decision to not investigate, or stop investigating on this ground, the principal officer or their delegate should consider the amount and quality of the information provided and whether the discloser's involvement in the investigation is critical. If other possible witnesses can be identified, or an investigation can be conducted by examining documents or electronic records, this should occur, so long as that type of investigation is practicable.

It may also be appropriate to consider whether one of the other grounds for not investigating apply, such as whether the disclosure concerns serious disclosable conduct (see 6.2.2) or whether the disclosure is frivolous or vexatious (see 6.2.3).

6.2.6.2 Discloser unable or unwilling to assist in the investigation

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if an investigation is impracticable because the discloser refuses, fails or is unable to give the investigator the information or assistance (s 48(1)(i)(ii)). For this ground, the investigator must have actually requested information or assistance from the discloser, and the lack of that information or assistance must make it impracticable to investigate the disclosure.

All public officials, including the discloser, have an obligation to use their best endeavours to assist in a PID investigation (see 4.4 of this guide). However, depending on the circumstances, including the seriousness of the matter, it may nevertheless be reasonable for the discloser not to wish to assist in the investigation. As discussed in 6.2.6.1 above, the principal officer or delegate should consider whether the discloser's involvement in the investigation is critical, and whether there are other sources of information available for the investigation.

6.2.6.3 The age of the information

The principal officer or their delegate may decide not to investigate a disclosure (or stop investigating it) if an investigation is impracticable because of the age of the information (s 48(1)(i)(iii)).

There is no time limit for making a disclosure (see 2.5.3 of this guide). However, if the disclosure relates to matters that occurred a long time ago, it may be difficult to locate and interview witnesses and relevant records may have been destroyed. Mere difficulty in conducting an investigation would not be sufficient to meet this ground. The principal officer or their delegate should consider what evidence is required and whether it is possible or practicable to access it. It may also be appropriate to consider whether one of the other grounds for not investigating apply, such as whether the disclosure concerns serious disclosable conduct (see 6.2.2).

6.3 DOES A DECISION NOT TO INVESTIGATE PREVENT OTHER ACTION?

A decision not to investigate, or investigate further, under the PID Act does not prevent any other type of investigation of the matter (s 48(2)).

For example, a disclosure might be made about an alleged breach of the Code of Conduct under the Public Service Act. If the requirements for making an internal disclosure were met, the discloser would be given protection under the PID Act. However, the principal officer or their delegate might determine that the alleged wrongdoing is not 'serious disclosable conduct', meaning it is not sufficiently serious to warrant investigation under the PID Act. Nonetheless, the allegation may still warrant investigation under the Code of Conduct procedures in force under the Public Service Act, and the information can be referred for handling under those procedures.

It should be noted that in the scenario above, the decision not to investigate cannot be made on the grounds discussed in 6.2.4.2 of this guide, as there is no current or prior investigation of the disclosure. If none of the grounds in s 48 apply, it is necessary for the principal officer to complete their investigation under the PID Act.

In 7.3.4 of this guide we explain how the PID investigation can be integrated with, and complement other investigation processes.

6.4 WHAT RECORDS MUST BE MADE OF A DECISION NOT TO INVESTIGATE?

The principal officer or their delegate should make a written record of their decision not to investigate a disclosure. In practice, those written reasons may be recorded as part of the notice given to the discloser (see 6.5 of this guide).

The principal officer or their delegate may decide during a PID investigation that it is inappropriate to continue the investigation on one of the grounds in s 48. If so, they are not obliged to complete the PID investigation and prepare a report under s 50 of the PID Act. They must, however, prepare written reasons for their decision under s 48 of the PID Act and notify the discloser, and the Ombudsman or IGIS (see 6.5 of this guide).²¹

6.5 WHO MUST BE NOTIFIED OF A DECISION NOT TO INVESTIGATE?

Once the principal officer or their delegate decides not to investigate a disclosure under one of the grounds in s 48 of the PID Act, they must notify:

- » the discloser (see 6.5.1 of this guide)
- » the Ombudsman (see 6.5.2 of this guide), or
- » the IGIS, if the disclosure was allocated to one of the intelligence agencies (see 6.5.2).

6.5.1 Notifying the discloser

The principal officer or their delegate must notify the discloser of a decision not to investigate their disclosure, or to stop investigating it (s 50(1)(b)). The notice must be in writing.

The notice of allocation of the disclosure and the decision not to investigate it may be given to the discloser in the one document (s 50(4)). However, this should only be done if the two decisions are close in time (see 5.2.5.3 of this guide).

The notice must contain the reasons for the decision not to investigate the disclosure and any other action the discloser may be able to take under other Commonwealth laws to address the information they have disclosed (such as in relation to a workplace grievance) (s 50(2)).

²¹ Forms to notify the Ombudsman of the allocation of a PID are available on the Ombudsman's website at www.PID.ombudsman.gov.au.

The principal officer or their delegate may delete from the reasons given to the discloser any reasons that would cause the document to (s 50(3)):

- » be exempt for the purposes of Part IV of the FOI Act
- » have, or be required to have, a national security or other protective security classification, or
- » contain intelligence information (see 2.7.51 of this guide).

It is possible that in a single public interest disclosure, there are a number of allegations of disclosable conduct. The principal officer or their delegate may decide to continue investigating some conduct and not investigate, or cease investigating, others under s 48. It is important that those matters that are not investigated in the PID investigation are dealt with in a s 48 notice of a decision to not investigate, and that the remaining matters are dealt with in the report on the investigation (s 51).

6.5.1.1 What if the discloser cannot be contacted?

The discloser does not have to be notified of the decision not to investigate their disclosure if it is not reasonably practicable to contact them (s 50(5)). However, the principal officer or their delegate should still make a written record of their decision and the reasons for it (see 6.4 of this guide). A written record should also be made of the reasons why contacting the discloser was not practicable and the date, time and method of any efforts to contact the discloser.

6.5.2 Notifying the Ombudsman or IGIS

The principal officer or their delegate must inform the Ombudsman when they make a decision to not investigate a disclosure, or to stop investigating a disclosure. The notice must include the reasons for that decision (s 50A(1)). The intelligence agencies are obliged to inform the IGIS, rather than the Ombudsman(s 50A(2)).

Agencies required to report to the Ombudsman may use the form published on the Ombudsman's website.²² The IGIS does not have a required format for notifications from the intelligence agencies.

²² Forms to notify the Ombudsman of the allocation of a PID are available on the Ombudsman's website at www.PID.ombudsman.gov.au.

7 Conducting an investigation

- 7.1 General requirement to investigate an internal disclosure
 - 7.2 What sort of investigation is required?
 - 7.3 Investigations under the PID Act
 - 7.4 After the investigation
 - 7.5 Some administrative considerations
-

7.1 GENERAL REQUIREMENT TO INVESTIGATE AN INTERNAL DISCLOSURE

The principal officer may delegate any of their functions or powers to a public official who belongs to their agency (s 77). This includes delegating the function of investigating a disclosure.

Section 47 of the PID Act requires the principal officer of an agency or their delegate to investigate a disclosure allocated to that agency for handling under the PID Act. The exception is where the principal officer or their delegate decides not to investigate the disclosure under s 48 of the PID Act. Section 6 of this guide explains the circumstances in which a decision not to investigate may be made and the associated notification requirements.

This chapter explains the formal procedural requirements for conducting an investigation under the PID Act. It does not explain the actual process of investigating a disclosure, although some of the pitfalls to avoid are highlighted in 7.8 of this guide.

7.1.1 Initial advice to the discloser about the investigation

The investigator should check whether the discloser has already been informed about the principal officer's powers to investigate the disclosure (see 6.1.1 of this guide). That advice should be provided to the discloser within 14 days after the disclosure is allocated to the agency for handling under the PID Act, if it is reasonably practicable to do so (s 50(1)).

The investigator must also advise the discloser of the estimated length of their investigation (s 50(1A)). This is an important part of managing the discloser's expectations (see 7.5.1 of this guide). The PID Act requires an investigation to be completed within 90 days of allocation (see 7.3.3.1 of this guide). If a longer time is required, the agency should seek an extension of time from the Ombudsman (or IGIS, if the agency is one of the intelligence agencies) (see 9.1.4 of this guide).

7.2 WHAT SORT OF INVESTIGATION IS REQUIRED?

An internal disclosure may be investigated in one of two ways:

- » under a separate investigate power (see 7.2.1 of this guide).
- » under the PID Act (see 7.3 of this guide).

7.2.1 Investigations under a separate investigative power

Investigation under a 'separate investigative power' is only relevant for disclosures allocated to the Ombudsman, IGIS or a prescribed investigative agency.²³ For disclosures allocated to all other agencies, refer to 7.3 of this guide.

7.2.1.1 What is a separate investigative power?

If the disclosure has been allocated to the Ombudsman, IGIS or a prescribed investigative agency,²⁴ they may use their own separate investigative powers rather than investigating under the PID Act (s 49(1)). For example, the Ombudsman has powers to investigate under the *Ombudsman Act 1976*, and the IGIS has powers under the *Inspector-General of Intelligence and Security Act 1986*. The circumstances in which the Ombudsman or IGIS will investigate are set out in 9.1.3 and 9.2.1 of this guide.

7.2.1.2 Effect of using a separate investigative power

Conducting the investigation under a law other than the PID Act does not alter the protections for the discloser (see part 8 of this guide). The confidentiality provisions in the PID Act also continue to apply (see 7.4 of this guide), as well as any confidentiality provisions in the legislation under which the investigation is conducted.

The time limits and reporting provisions discussed in 7.3.1 and 7.3.5 of this guide do not apply to an investigation conducted under a separate investigative power. The investigation, including the discretion not to investigate further, must be conducted in accordance with the legislation under which the agency is acting (such as the *Ombudsman Act 1976* in the case of the Ombudsman).

If the investigator suspects that information disclosed as part of an internal disclosure, or obtained during their investigation, is evidence of an offence against a Commonwealth, state or territory law, they may disclose that information to a member of a relevant police force (s 56(1)). Police notification is mandatory if the suspected offence is serious (that is, punishable by imprisonment for two years or more (s 56(2))). 7.3.6 of this guide provides further details about police notifications.

7.2.1.3 Notifying the discloser of the decision to investigate under a different law

If the Ombudsman, IGIS or prescribed investigative agency decides to investigate a disclosure under a separate investigative power, they should notify the discloser accordingly. That notice should explain that the discloser remains entitled to the PID Act protections, even though the disclosure is being investigated under a different law.

7.3 INVESTIGATIONS UNDER THE PID ACT

7.3.1 What does it mean to 'investigate' under the PID Act?

The purpose of a PID investigation is to establish whether one or more instances of disclosable conduct have occurred (s 47(1)). The starting point of the investigation is the information provided by the discloser. However, the investigator may also consider whether the information they obtain during the investigation indicates that there are other, or different instances of disclosable conduct (s 47(2)).

During the PID investigation, the investigator should consider whether it is appropriate for the subject matter of the disclosure to be investigated under another law of the Commonwealth, or procedures established under another law of the Commonwealth (see 7.3.4 of this guide). The investigator should

²³ As explained in 2.7.3 of this guide, there are no prescribed investigative agencies at the time of publication.

²⁴ As explained in 2.7.3 of this guide, there are no prescribed investigative agencies at the time of publication.

also bear in mind that if one of the discretionary grounds in s 48 of the PID Act apply, it may be appropriate to discontinue the investigation under the PID Act (see 6.2 of this guide for more information about discontinuing a PID investigation).

There are time limits for the investigation (see 7.3.3.1 of this guide). At the conclusion of the investigation, the investigator prepares a written report of their investigation (s 51). The investigation is completed when the report is prepared (s 52(2)). The requirements of the PID investigation report are discussed in 7.3.5 of this guide.

7.3.2 Who should investigate?

The principal officer is responsible for conducting investigations, and may delegate the investigative function to an officer who belongs to their agency (s 77). The delegate could be a person already employed by the agency, or it could be a person contracted to conduct the particular investigation. 7.3.2.1 of this guide explains some of the considerations for a principal officers before delegating the PID investigation function to a person who is not ordinarily employed by the agency.

The investigator should have experience in conducting investigations into conduct of the type the disclosure is about.²⁵ Before commencing the investigation, they should become familiar with the PID Act, especially the confidentiality requirements and the protections for disclosers.

Investigators must ensure that they do not have an actual or perceived conflict of interest (for example, if information suggests they or a family member are implicated in the alleged wrongdoing). Unless there are other compelling reasons not to do so, the investigator should be separate from the workgroup where the alleged wrongdoing has occurred.

7.3.2.1 Delegating the investigative function to a contractor

The delegation of the principal officer's investigative function to a person external to the agency may be appropriate and necessary for the proper handling of a PID matter. For example, where the handling of a PID requires a special set of skills or expertise, the principal officer may wish to delegate some powers or functions to an appropriately qualified or experienced person. An external investigator may also be necessary to effectively manage the risk of real or perceived bias or conflict of interest in the handling of a particular matter.

When engaging an external contractor to conduct an investigation, the principal officer should consider confining their delegation of the investigation power in s 53 by specifying terms of reference for the investigation, for example, by personally identifying the investigator and setting out clearly the scope of the investigation. This could include the issues that the investigation should cover and whether the investigator is to prepare the report under s 51 of the Act and particular actions that should be taken. This should be supported by the terms of the contract entered into with the contractor.

7.3.3 PID investigation requirements

A PID investigation is conducted as the principal officer, or their delegate, sees fit (s 53), subject to the need to comply with the PID Standard (s 74). There are also special mandatory requirements for investigations into possible fraud (see 7.3.4.1 of this guide) or a possible breach of the Codes of Conduct which apply to employees of the Australian Public Service, or Parliamentary Service (see 7.3.4.2 of this guide).

²⁵ The PID investigation requirements are discussed from 7.3.3 onwards.

7.3.3.1 *Time limit for investigations*

Investigations under the PID Act must be completed within 90 days of the date the disclosure was allocated for investigation (s 52(1)). Agencies that investigate public interest disclosures under another law (the Ombudsman, IGIS and prescribed investigative agencies) are not bound by the time limits in the PID Act, but rather by the legislation under which they investigate.

The PID investigation is complete when a report of the investigation is prepared. If an agency is unable to complete the investigation within the usual 90 day period, the Ombudsman, or the IGIS in the case of intelligence agencies, may grant one or more extensions of time. The requirements for an extension of time are discussed in 9.1.4 of this guide.

Exceeding the time allowed under the PID Act does not invalidate the investigation. The agency remains obliged to complete the PID investigation and prepare a report. However, if the investigation is not completed within 90 days, or such longer period as granted by the Ombudsman or IGIS, the discloser may be entitled to make an external disclosure under the PID Act (see 2.7.7 of this guide).

7.3.3.2 *An administrative investigation*

An investigation under the PID Act is an administrative investigation. This means that the person conducting the investigation must comply with administrative law principles of general application such as procedural fairness (7.3.3.8 of this guide). However, s 53 of the PID Act provides considerable latitude to an investigator to decide how to conduct the investigation, provided they comply with the PID Standard (7.3.3.3 of this guide) and, if relevant, observe the special requirements relating to fraud investigations (7.3.4.1 of this guide) and Code of Conduct investigations (7.3.4.1 of this guide).

The formality of the investigation should be commensurate with the seriousness and nature of the alleged disclosable conduct and the importance of the particular evidence. The investigator's records should contain sufficient detail appropriate to the nature of the investigation (7.5.2 of this guide).

General guidance for investigators can be found in the Australian Government Investigation Standards 2011 (AGIS), issued by the Attorney-General.²⁶ The AGIS sets out minimum standards that must be followed by non-corporate Commonwealth entities when investigating fraud. However, it also has useful information on such topics as investigation planning, interviewing witnesses and finalising investigations that can be applied to investigations more generally.

Investigators may also find it helpful to refer to the Administrative Review Council's Best Practice Guides on aspects of administrative decision-making, including natural justice requirements (also known as 'procedural fairness'), assessing evidence and decision writing, available at www.arc.ag.gov.au.

7.3.3.3 *PID Standards for conducting investigations*

Part 3 of the PID Standard (ss 8-12) sets out mandatory requirements for PID investigations. These apply to all investigations under the PID Act (s 8, PID Standard). The modified requirements for fraud investigations under the PID Act are discussed in 7.3.4.1 of this guide.

The requirement to provide information to the discloser about the principal officer's power to investigate is described in 7.1.1 of this guide (s 9, PID Standard).

²⁶ A copy of the Australian Government Investigation Standards 2011 is published on the website of the Attorney-General's Department at <http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/AGIS%202011.pdf>

Discussed below are the PID Standard requirements for:

- » interviewing witnesses (see 7.3.3.5 of this guide)
- » standard of proof (see 7.3.3.6 of this guide)
- » the evidence that can be taken into account (see 7.3.3.7 of this guide).

7.3.3.4 What legal power does the investigator have to obtain information?

When investigating a disclosure, the investigator may obtain information from such persons and make such inquiries as they think fit (s 53(2)). All current public officials are obliged to use their best endeavours to assist the principal officer, or their delegate, in a PID investigation (s 61(1)). The investigator may wish to draw this obligation to the attention of any public official or contractor who is reluctant to provide information or answer questions relevant to the investigation. The PID Act does not give investigators any powers to compel witnesses to attend interviews, answer questions or produce documents. However, a principal officer may be able to rely upon other legislation to obtain the cooperation of staff members (for example – legislation relating to a person’s employment responsibilities).

It is permissible for an investigator, or an official assisting with a PID investigation, to disclose, record or use information in connection with that investigation that would otherwise be protected by secrecy or confidentiality provisions in most Commonwealth laws, unless that would breach a designated publication restriction²⁷ (s 75(1)) or some other Commonwealth law enacted after 15 January 2014 and which expressly prevails over s 57 of the PID Act.

In the case of intelligence information obtained in the course of a disclosure investigation, it is recommended that the investigator contact the relevant intelligence agency and/or the IGIS, to discuss how that information should be protected and, if necessary how that information might be further investigated.

In some cases, it will be possible to investigate an internal disclosure by obtaining and examining existing agency records. The investigator may also seek general background information (e.g. advice from a business line about the agency’s usual processes, or copies of written procedures). This can be done informally, without following the formal requirements for conducting a PID interview.

However, it will usually be necessary for the investigator to obtain additional information from the discloser and other possible witnesses. This could be done by way of a list of written questions, or in an interview conducted by telephone or in person. Whether in writing or in person, the PID Investigator’s requests for specific information from an individual should be regarded as an interview in connection with a PID investigation. Those interviews are subject to some specific requirements, discussed in 7.3.3.5 of this guide.

7.3.3.5 Interviewing a witness (including the discloser)

As discussed in 7.3.3.4 above, the PID investigator may obtain information from such persons and make such inquiries as they think fit. This can include seeking further information from the discloser. If the investigator decides to conduct an interview seeking specific information from a person for the purposes of the PID investigation, they must comply with s 10 of the PID Standard. These requirements apply even if the interview is conducted in a relatively informal way, for example, by telephone. They should also be followed when an investigator decides to seek information from a person in the form of written answers to questions, whether those questions are asked orally, or in writing.

²⁷ A ‘designated publication restriction’ means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the Family Law Act 1975 and the Migration Act 1958), witness protection and law enforcement mechanisms (see the full definition in s 8).

The person being interviewed must be informed of the following (s 10(1), PID Standard):

- » the name of any person conducting the interview, (including anyone who may be present in an assisting or record keeping capacity)
- » the function that each of the people present is performing in the investigation,
- » that the principal officer is required to investigate a disclosure to establish whether there has been disclosable conduct
- » the legal authority for the investigator to conduct the investigation (for example, where the principal officer's investigative function under the PID Act has been delegated)
- » general information about the process of conducting a PID investigation, including confidentiality requirements and protection of the discloser's identity.

The person being interviewed should also be advised of the protections they have under s 57 of the PID Act in relation to the information they provide at the interview (s 10(1)(d), PID Standard). In summary, s 57 provides immunity for the act of providing relevant information or producing relevant document when asked to do so by a PID investigator (see s 8.3.1 of this guide).

All interviews should be conducted in private. The people present at any interview should be limited to those people whose presence is necessary for conducting the interview. Those who are interviewed should be advised that information about the matter is confidential, that release of information may jeopardise an investigation and that they may be committing an offence if they divulge any information that is likely to identify the discloser. See 7.3.3.9 of this guide for more information about the confidentiality of the investigation.

The investigator should keep written records of the interview (see 7.5.2 of this guide). Audio or visual recordings of the interview must not be made without the prior knowledge and consent of the person being interviewed (s 2(a), PID Standard).

At the conclusion of the interview, the investigator should ask the person if they wish to make a final statement or comment, or express a position about the matters being investigated (s 2(b), PID Standard). The person's response, and any final statement or comment they make must also be included in the record of interview (s 2(c), PID Standard).

7.3.3.6 Standard of proof

The standard of proof in a PID investigation is the civil standard: a fact is only taken to be proved if there is sufficient evidence to prove it 'on the balance of probabilities' (s 11, PID Standard). This means that the principal officer, or their delegate, cannot make a finding that there has been disclosable conduct unless they are satisfied on the basis of the evidence gathered during the investigation that it is more likely than not that the disclosable conduct occurred.

It is not necessary for the principal officer to positively identify a person or persons responsible for the conduct. It is enough to be satisfied that the conduct was engaged in by an official belonging to the agency, or the agency more broadly. 7.3.6 of this guide explains what action is required if the investigator concludes that there is evidence of the commission of a criminal offence.

7.3.3.7 Evidence

The evidence relied upon in a PID investigation must be relevant (s 12(2), PID Standard).

The investigator must not place any weight on information they might obtain during the investigation unless it is of consequence to one of the matters under investigation and tends to make it more or less probable that a relevant fact exists. Any finding of fact in a PID investigation must be based on logically probative evidence (s 12(1), PID Standard).

7.3.3.8 Procedural fairness

In an administrative investigation the investigator must ensure that a person against whom allegations are made is accorded procedural fairness (also known as 'natural justice'). If adverse information comes to light about others in the course of the investigation those person are also entitled to procedural fairness. This could include the discloser.

What procedural fairness requires varies with the circumstances, but essentially it means that the person is entitled to:

- » have a decision-maker act fairly and without bias
- » know the substance of allegations and evidence against them if an adverse finding is going to be made about their conduct
- » have a reasonable opportunity to respond.

The requirement to provide the person with an opportunity to respond to an allegation about them only arises at the point where it is likely that an adverse finding is to be made about their conduct. This means that a person does not need to be told about allegations made about them that the agency decides are of no substance (for example if the agency decides not to investigate a disclosure, or stop the investigation, on the basis that the disclosure is clearly frivolous or vexatious). However, see 7.4.1 of this guide for information about when it is appropriate to notify a person of the outcome of an investigation about them.

7.3.3.9 What must the official who is the subject of the disclosure be told?

The PID Act does not require the investigator to give a copy of a public interest disclosure to the person who is the subject of that disclosure, or tell them the identity of the person who made the disclosure. The information that the subject of the disclosure is entitled to be told will depend upon what is necessary to investigate the allegations in a way that observes procedural fairness.

Given the special protection of the discloser's identity in the PID Act, it is appropriate to protect the discloser's identity as far as possible, unless identifying them is necessary for the purposes of investigating the disclosure or the discloser has consented to being identified (see 7.3.3.9). Protecting the discloser's identity is discussed further in 8.1 of this guide.

Procedural fairness does not mean that a person must be told about any allegations made about them as soon as the disclosure is received or an investigation is commenced. There may be good reasons to carry out certain investigations before interviewing a person who is suspected of wrongdoing, particularly if there are concerns that they may collude with others or evidence may be destroyed if they are alerted.

A person who is subject to allegations of wrongdoing should be given information about their rights and obligations under the PID Act, and about the agency's investigation procedures and any other relevant matter, such as Code of Conduct proceedings. A key principle to bear in mind is that anyone who is subject to an allegation or an investigation is innocent of any wrongdoing until proven otherwise, and they may be completely exonerated.

Agencies should consider support for any official who is the subject of an allegation made in a public interest disclosure. They are likely to find the experience very stressful. It is appropriate to ensure that they know how to access employee assistance programs or other support (including legal advice) if they need it.

7.3.3.10 Ensuring confidentiality of the investigation

Agency procedures must provide for confidentiality of investigative processes (s 59(1)(b)).

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 the information (s 65(1)) unless one of the following exceptions apply s 65(2):

- » the disclosure or use of the information is for the purposes of the PID Act or in connection with the person's powers and functions under the PID Act
- » the disclosure or use is for the purposes of, or in connection with, taking action in response to a disclosure investigation
- » the information has previously been lawfully published and is not intelligence information, or if it is intelligence information, the principal officer of the source agency for the information has consented to the disclosure or use (s 65(2)).

To satisfy these confidentiality requirements, and to minimise the possibility of detrimental action against the discloser and others, including witnesses, agencies should establish a secure record system to deal with internal disclosures. Agencies should ensure that:

- » all paper and electronic documents and files are secure and only able to be accessed by authorised officers, investigators and other officers involved in managing the disclosure
- » other materials such as interview tapes are stored securely with access only by officers involved in handling the disclosure
- » communications and documents relating to the investigation are not sent to an email address to which other staff have access or to a printer or fax machine in an open area.

The identity of a person who is the subject of allegations or an investigation should be protected as much as practicable. Information that identifies them should only be passed to those involved in the investigation or in taking other necessary action under the PID Act (such as action to minimise the risk of reprisal against the discloser).

7.3.4 Is a different type of investigation appropriate?

Once the investigator has investigated the disclosure sufficiently to reach a conclusion that one or more instances of disclosable conduct may have occurred, they may decide that it would be more appropriate for the matter to be dealt with under another Commonwealth law. That further investigation, or reinvestigation, may be conducted by another person within the same agency, or by another appropriate body under a Commonwealth law other than the PID Act, (s 47(3)).

Concluding a PID investigation and referring the information to be dealt with under another law is not the same as making a decision to stop investigating a disclosure on the basis that the information has already been investigated, or another investigation is already under way (see 6.2.4 of this guide).

Some examples of other types of investigations that might be appropriate at the conclusion of a PID investigation are listed in 6.2.4.3 of this guide. See also 7.3.4.1 and 7.3.4.2 below, for information about investigating alleged fraud, or a possible breach of a Code of Conduct.

If another type of investigation is appropriate, the PID investigation may conclude at that point. The PID investigator must prepare a report of their investigation (see 7.3.5 of this guide). The report should include details of what action has been taken, or will need to be taken, to refer the information on to be dealt with under that other law or procedure.

It is legally permissible for an agency to conduct the entire investigation under the framework of the PID Act, and this may be convenient and efficient in some cases. However, it is generally preferable for the PID investigation to be completed, with a report that recommends a separate, and subsequent investigation, such as a fraud or Code of Conduct investigation. This avoids the confusion of two sets of legal requirements applying to the combined investigations. It is also likely that the more formal requirements of a Code of Conduct or fraud investigation will make it difficult to complete the combined investigation within the usual 90 day time frame for a PID investigation (see 7.3.3.1 of this guide).

7.3.4.1 Investigation of alleged fraud

The effect of s 21 of the *Public Governance, Performance and Accountability Act 2013* and the Commonwealth Fraud Control Policy is to require all non-corporate Commonwealth entities to comply with the Australian Government Investigations Standards (AGIS) when conducting investigations into fraud against them, or relating to the programs and legislation they administer.²⁸ The AGIS sets out minimum case handling standards for fraud investigations, including minimum training requirements for investigators and requirements for conducting interviews and preparing briefs of evidence.

If the principal officer of a non-corporate Commonwealth entity is investigating a disclosure that concerns alleged fraud against the Commonwealth, the PID investigation must also comply with the Commonwealth Fraud Control Policy and the AGIS(s 53(4)). If there is any inconsistency between the requirements of the Commonwealth Fraud Control Policy and the requirements of the PID Act and PID Standard, the PID requirements must be followed. However, it should be noted that when a PID investigation relates to fraud, Part 3 of the PID Standard (which deals with the conduct of interviews for a PID investigation) applies only to the extent that it is not inconsistent with the Commonwealth Fraud Control Policy (s 8(2), PID Standard).

Given the complexity of concurrently complying with the requirements of the PID Act and PID Standard, and the Commonwealth Fraud Control Policy, the recommended course of action when investigating disclosure of alleged fraud is as discussed in 7.3.4 above.

The person investigating the disclosure (whether that be under the PID Act, and/or the Commonwealth Fraud Control Policy and the AGIS) should be aware of their obligation to notify the police of information that they suspect on reasonable grounds is evidence of a serious criminal offence (see 7.3.6 of this guide).

7.3.4.2 Investigation of disclosure about a possible breach of a Code of Conduct

- » When investigating a disclosure concerning an alleged breach of the Code of Conduct under the *Parliamentary Service Act 1999*, the principal officer must comply with the procedures established under s 15(3) of that Act.
- » When investigating a disclosure concerning an alleged breach of the Code of Conduct under the *Public Service Act 1999*, the principal officer must comply with the procedures established under s 15(3) of that Act (s 53(5)).

When investigating a disclosure concerning a possible breach of one of these Codes of Conduct, the principal officer or their delegate would initially investigate the disclosure under the PID Act to assess if there is any substance to the allegation of misconduct. If the principal officer decides that there is insufficient prima facie evidence of a breach of the relevant Code of Conduct arising from the disclosure, or does not wish to impose the sanctions available under s 15 of the relevant Act, the PID investigation can be finalised at this point. The principal officer must prepare a report (see 7.3.5 of this guide) that records their reasons for reaching this conclusion.

²⁸The Commonwealth Fraud Control Policy and the AGIS are both published on website of the Attorney-General's Department at: <http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx>

If the principal officer decides that the disclosure investigation has revealed sufficient prima facie evidence of a breach of the APS Code of Conduct, they should consider whether a different investigation should be conducted under another law of the Commonwealth (s 47(3)). A Code of Conduct investigation in accordance with an agency's s 15(3) procedures is another law of the Commonwealth for this purpose.

The principal officer, or their delegate, may decide to finalise the PID investigation at the point where they are satisfied that there is sufficient evidence to start a Code of Conduct investigation under the agency's procedures under s 15(3) of the relevant act. The principal officer may then prepare a report under s 51 of the PID Act, recording a decision or recommendation that a Code of Conduct inquiry commence. Alternatively, the Code of Conduct investigation may be completed as part of the overall PID investigation, however as discussed, above the investigator must comply with both the Code of Conduct and PID investigation requirements. This includes the requirement under s 51 of the PID Act to prepare a report of the (combined) investigation (see 7.3.5 of this guide).

7.3.5 PID investigation report

After an internal disclosure has been investigated, the principal officer, or their delegate, must prepare a written report of the investigation (s 51(1)). The PID investigation is only completed when the principal officer has prepared the report (s 52(1)).

The report is the agency's record of the investigation of the disclosure and the action to address any disclosable conduct that was found to have occurred. Additionally, the investigation report is a record of the agency's response to any claims of detriment against the discloser (see 7.3.5.1 of this guide).

The PID investigation report must state (where relevant):

- » the matters considered in the investigation (s 51(2)(a)), including (s 47(2)):
 - the disclosable conduct alleged by the discloser
 - any other possible disclosable conduct subsequently identified
- » how long the investigation took (s 51(2)(b)), that is, the number of days between allocation and the date the report was prepared (s 52)
- » the steps taken to gather evidence (s 13(c), PID Standard)
- » a summary of the evidence (s 13(d), PID Standard)
- » principal officer's findings, based on that evidence (s 51(2)(c) and s 13(d), PID Standard), including:
 - whether there was any disclosable conduct, and if so, what type (s 13(a), PID Standard)
 - the laws, rules procedures etc to which that disclosable conduct relates (s 13(b), PID Standard)
- » any action taken, or currently in train to address those findings (s 51(2)(d))
- » recommendations about other action to address those findings (s 51(2)(d))

The action to address the findings of the PID investigation could include a different type of investigation (see 7.3.4 above) or referral of the matter to the police (see 7.3.6 below).

If the investigation was inconclusive in any respect, the report should say so and explain why.

If parts of the disclosed information were not investigated, the report should explain the reasons for the decision not to investigate those matters (see 6.2 of this guide for information about the reasons that may be used to decide to stop investigating a disclosure).

7.3.5.1 *Detrimental action against the discloser*

The PID investigation report must also detail whether there were any claims, or evidence, of detrimental action against the discloser, and how the agency responded to them (s 51(2)(e)).

The PID investigation report must include the following information (s 51(2)(e)):

- » any claims made about detrimental action taken against the discloser
- » how the agency responded to those claims (e.g. investigation, support or protection for the discloser)
- » whether the agency found any evidence of detrimental action against the discloser (not limited to detrimental action identified by the discloser)
- » the action taken or recommended to address any findings of detrimental action against the discloser.

The person preparing the PID investigation report should consult with the authorised officer who allocated the disclosure and any person who was involved in the initial risk assessment for the discloser (see 5.3 of this guide) to ensure that they have all the relevant information to complete this part of the report. If a support person was appointed for the discloser, that support person should also be consulted.

7.3.5.2 *Findings of fact*

Any finding of fact in the report must be based on relevant evidence, sufficient to satisfy the principal officer or their delegate on the balance of probabilities of the existence of that fact (see 7.3.3.6 and 7.3.3.7 of this guide). Given the purpose of the PID investigation (to discern if there are one or more instances of disclosable conduct – s 47(2)), the primary finding to be made is whether there is one or more instances of disclosable conduct (see 7.3.1 of this guide). The report should also make a finding regarding any claims of detrimental action against the discloser.

7.3.5.3 *Copy for the discloser*

The principal officer must give a copy of the PID investigation report to the discloser within a reasonable time of preparing it (provided that contacting the discloser is reasonably practicable) (s 51(4)).

The copy of the report given to the discloser may have some information deleted if it is likely to enable the identification of any person (the discloser or another person, such as someone who is under investigation), or if including the information would cause the document to:

- » be exempt under the FOI Act (exempt material includes commercially valuable information, material obtained in confidence, Cabinet information, personal information whose disclosure would be unreasonable and contrary to the public interest, and information that could prejudice an investigation or affect the effectiveness of agency audit procedures)
- » have a national security or protective security classification, or
- » contain intelligence information or sensitive law enforcement information.

7.3.6 Criminal matters

7.3.6.1 *Notifying the police*

If an investigator suspects that information disclosed as part of an internal disclosure, or obtained during their investigation of a disclosure, is evidence of an offence against a Commonwealth, state or territory law, they may disclose that information to a member of a relevant police force (s 56(1)).

Police notification is mandatory if the suspected offence is serious (that is, punishable by imprisonment for two years or more (s 56(2))).

Notification to the police under s 56 of the Act does not of itself mean that the PID investigation can or should stop. The police will assess the reported information and decide whether and how to investigate it in accordance with their usual operational priorities. The principal officer or their delegate must still consider whether other administrative or disciplinary action is also appropriate in response to the conduct, consistent with the integrity arrangements for the agency concerned and given the position of the official whose conduct is in question. Dialogue with the police will be important to ensure that whatever action the agency takes does not prejudice a criminal investigation or prosecution. In any case, the PID investigation will not be complete until the principal officer prepares their report under s 51 (see 7.3.5 of this guide).

In most cases, the suspected offence will be a crime under a Commonwealth or ACT law. If so, the information should be referred to the Australian Federal Police (AFP). The AFP's website contains information about the procedure for government agencies to make reports, and contact details for initial enquiries or pre-referral advice.²⁹ However, depending on the particular offence involved, it may be appropriate to refer the information to a police force of an Australian state or territory.

Section 56 also applies where an investigative agency conducts a PID investigation using a 'separate investigative power' (see 7.2.1 of this guide) and in the case of an investigation of a disclosure under an agency's procedures relating to fraud (see 7.3.4.1 of this guide).

7.3.7 What impact can investigations have on the workplace?

If an investigation becomes generally known to staff (as is likely once interviews commence) people's reactions can vary considerably. Some staff may welcome action being taken, while others may not. As a result, workplace tensions may arise.

Managers can help by keeping the channels of communication open, while maintaining confidentiality as far as practicable. If the discloser's confidentiality has already been compromised, managers may:

- » let staff know that information about disclosable conduct has been provided
- » allow staff to air their feelings
- » provide information about the PID Act and agency procedures
- » indicate when further information is likely to be available.

See 8.5 and 8.6 of this guide for information about supporting and protecting officials.

7.4 AFTER THE INVESTIGATION

7.4.1 What should a person be told if allegations were made against them?

If the allegations in a disclosure have been investigated and the person who is the subject of them is aware of the allegations or that there has been an investigation, that person should be formally advised of the outcome of the investigation as it relates to them. It should be noted that this is not a procedural fairness requirement, and the person is not entitled to be told who made the disclosure (see 7.3.3.8 of this guide).

Agencies should consider how they will support the subject of a disclosure when allegations, which may have been publicly disclosed, are shown to be clearly wrong or unsubstantiated.

²⁹ <http://www.afp.gov.au/what-we-do/referrals>

7.4.2 What action does an agency need to take?

What happens at the end of an investigation will vary with the circumstances. The principal officer must take appropriate action in response to recommendations and other matters contained in the investigation report. Actions might include:

- » commencing Code of Conduct proceedings under the Public Service Act or another disciplinary process
- » referral of the matter to the police or another body that can take further action
- » mediation or conciliation of a workplace conflict
- » an internal audit or other review of an issue or the operations of a particular unit
- » implementing or changing policies, procedures or practices
- » conducting training and awareness sessions for staff.

7.4.3 What happens if the disclosure is not substantiated?

There may be a number of reasons why a public interest disclosure is not substantiated, including insufficient evidence to find on the balance of probabilities that any disclosable conduct occurred. The discloser should be given as much information as possible about the outcome of the investigation consistent with confidentiality limitations, and be assured that it does not mean that making a disclosure was not worthwhile. The information the discloser provided may be useful in making the agency aware of possible gaps in its policies or procedures, or lead to consideration of how to prevent similar issues in the future.

Regardless of the outcome, the discloser should be assured that they will still be protected under the PID Act for making a disclosure and that the agency will continue to support them.

7.4.4 What if the discloser is not satisfied with the agency's action?

A person who has made an internal disclosure may be unhappy with the agency's decision not to investigate a matter. If the disclosure is investigated, they may believe that the investigation or the agency's response to the investigation was inadequate. A reasonable belief that an investigation under the PID Act was inadequate or that the agency's response was inadequate is one of the conditions for making an external disclosure (see 2.7.7 of this guide).

A discloser who is unhappy with the process or how they have been treated may also complain to the Ombudsman (or the IGIS in the case of intelligence agencies). Agencies may want, therefore, to consider review or reconsideration measures to address situations where a discloser is not satisfied with the agency's handling of an internal disclosure.

In order to manage those possibilities well, it is important to manage the discloser's expectations from the outset. The information provided to the discloser at the time the disclosure is received; upon allocation; and during an investigation should be clear about the fact that once an official has made an internal disclosure, it is up to the agency to determine how best to resolve matters by identifying problems and taking corrective action.

It is also important that explanations given to the discloser at the end of the investigation are as comprehensive as possible, allowing for privacy and confidentiality considerations. The discloser needs to feel that the agency values their contribution in bringing the matter to their attention. Disclosers should be encouraged to approach the agency if they wish to discuss concerns about the process or the outcome. Agency procedures and all notice of decisions relating to the disclosure should nominate who to contact in that case.

7.5 SOME ADMINISTRATIVE CONSIDERATIONS

7.5.1 Keeping the discloser informed

A discloser can easily become concerned or dissatisfied if they feel they are being left in the dark or that nothing is happening. The PID Act requires the discloser to be notified at various stages in the process, provided the person's contact details are available. The discloser must be advised:

- » when the disclosure is either allocated for investigation, or not allocated because it has been determined not to be an internal disclosure
- » of information about the principal officer's discretionary powers to not investigate within 14 days of the disclosure being allocated (s 9 of the PID Standard)
- » if the agency decides to investigate
- » if the investigation is under the PID Act, the estimated length of the investigation
- » if the agency decides not to investigate, the reasons for the decision and any action that might be available to the discloser under other Commonwealth laws
- » if an investigation is conducted under the PID Act and an extension of time is granted by the Ombudsman or IGIS, the progress of the investigation
- » after the investigation report is completed.

Apart from the legislative requirements, the agency should keep the discloser up to date with reasonable information on what is being done in response to their disclosure. Early in the process, an authorised officer should make sure the discloser understands:

- » what the agency intends to do
- » the likely timeframe for an investigation
- » the discloser's responsibilities (such as maintaining confidentiality)
- » how they will be updated on progress and outcomes
- » who to contact if they want further information or are concerned about reprisal.

Any questions or concerns the discloser raises should be addressed honestly and as soon as possible. If they have not heard anything within a reasonable period, they are entitled to ask for an update.

The agency should also inform the discloser if it becomes apparent during the investigation that it is likely to take longer than originally expected. If an extension of the investigation time is required (see 9.1.4), the agency should inform the discloser before applying to the Ombudsman or IGIS and provide an estimate of the date when the investigation will be completed.

The discloser can also be referred to:

- » the agency's public interest disclosure procedures
- » support networks or services
- » the guide for disclosers and this guide, available at www.pid.ombudsman.gov.au.

It is important to balance the requirement to inform the discloser with the need to maintain confidentiality in the investigative process. The authorised officer and investigator need to be careful not to release information if doing so will impact on anyone's safety, the ongoing investigation, or the confidentiality of anyone who is under investigation.

It is also important to remind disclosers that they do not 'own' the investigation of their disclosure. It is up to agencies to determine how best to resolve matters by identifying problems and taking corrective action.

After an investigation, the principal officer must ensure that a report is prepared and that appropriate action is taken by the agency.

7.5.2 Keeping records

Good records ensure that all action taken regarding the receipt and handling of a public interest disclosure is reviewable (including by the Ombudsman or IGIS)³⁰.

Details about how and when a public interest disclosure was made must be recorded and kept in a secure place. If the disclosure was made orally, it should be documented by the recipient and consideration should be given to asking the discloser to sign a record of the disclosure. Subsequent conversations where the disclosure is discussed should also be documented. Each disclosure should be registered and given a unique reference number. Details of the risk assessment of reprisal, allocation, the investigation, notifications to the discloser and others should also be kept. The records should be factual and free from unnecessary statements such as conjecture about the discloser's motives or personal opinion about the person(s) the disclosure concerns.

In addition to the requirement to notify the Ombudsman or IGIS whenever a disclosure is allocated, or a decision made not to investigate or to stop investigating a disclosure, agencies are required to provide to the Ombudsman certain information about disclosures they have handled for the purposes of the annual report under the PID Act (s 15, PID Standard). Information from the intelligence agencies for inclusion in the Ombudsman's annual report on the operation of the PID Act is coordinated by IGIS, who provides the Ombudsman with an aggregated report. See also 7.5.4 of this guide.

7.5.3 Freedom of Information requests


Section 82(2) of the PID Act provides that the PID Act does not detract from any obligations imposed on an agency or a public official by any other law of the Commonwealth. Documents associated with a public interest disclosure do not attract any special exemption from the operation of the FOI Act. Requests for access to documents under the FOI Act must be considered on a case by case basis. A range of exemptions may apply to certain agencies and to individual documents or parts of documents, particularly in relation to material received in confidence, personal information, operations of agencies, and law enforcement.

The principal officer should ensure that any agency officer handling freedom of information requests is aware of the confidentiality and secrecy provisions of the PID Act as they may apply to them, noting that s 20(3)(d) permits the use and disclosure of identifying information for the purposes of a law of the Commonwealth, such as the FOI Act. The confidentiality and secrecy provisions of the PID Act are not secrecy provisions for the purposes of s 38 of the FOI Act, however they may be a relevant consideration in applying certain exemptions including the public interest test for conditional exemptions. If a document originates from another agency including the Ombudsman or IGIS, the agency should contact that agency to seek their comment prior to making a decision to grant access.

7.5.4 Monitoring and evaluation

An agency should put in place an effective system for recording the numbers and types of public interest disclosures, the number of investigations, the outcomes (including agency action taken in response to investigation report findings and recommendations), and details of any support provided to a discloser and allegations of reprisal. Capturing data about the number of instances where a person has disclosed information to an authorised officer that was assessed not to meet the criteria for a PID, and the number of determinations under s 70 of the PID Act deem a person to be a public official will also assist agencies to measure the extent of PID activity.

³⁰ The *Administrative Decisions (Judicial Review) Act 1977* applies to decisions under the PID Act.



Much of this information will be needed to satisfy the principal officer's obligation to provide information to the Ombudsman for the annual report on the operation of the PID Act (s 76 and s 15 of the PID Standard) (see .7.5.2 of this guide). It will also help agencies to evaluate the effectiveness of their procedures and identify any systemic issues.

The agency may also wish to monitor the resources (financial and human) allocated to handling public interest disclosures, particularly in complex investigations. Once the procedures have been in place for some time, it may also be useful to survey staff about their awareness of, and trust in, the procedures, and the attitude of managers to the agency's process, so that improvements can be made.

8 Support and protection under the PID Act

- 8.1 Confidentiality**
- 8.2 Protection for the discloser**
- 8.3 Protection for witnesses in a PID investigation**
- 8.4 Officials exercising powers or performing functions under the PID Act**
- 8.5 Preventing and protecting from detriment and reprisal**
- 8.6 Practical support and protection strategies**
- 8.7 Access to court**
- 8.8 Reprisal is a crime**

The PID Act provides a means for protecting public officials, and former public officials, from adverse consequences of disclosing information that, in the public interest, should be disclosed (s 7(1)).

Supporting and protecting disclosers and other staff is an important agency responsibility that is key to successful implementation of the scheme. So too is maintaining an appropriate level of confidentiality.

8.1 CONFIDENTIALITY

Section 65 of the PID Act is a general secrecy provision that protects any information that a person obtains in the course of conducting a disclosure investigation, or in connection with the performance of a function, or exercise of a power under the PID Act. It therefore applies to authorised officers, PID investigators and any person performing any of the principal officer's functions under the PID Act (including, but not limited to a delegated power or function).

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 the information (s 65(1)) unless one of the following exceptions apply s 65(2):

- » the disclosure or use of the information is for the purposes of the PID Act or in connection with the exercise of the person's powers or performance of their functions under the PID Act
- » the disclosure or use is for the purposes of, or in connection with, taking action in response to a disclosure investigation
- » the information has previously been lawfully published and is not intelligence information, or if it is intelligence information, the principal officer of the source agency³¹ for the information has consented to the disclosure or use (s 65(2)).

The principal officer of each agency is obliged to establish procedures to provide for the confidentiality of the investigation process (s 59(1)(b)). See 7.3.3.9 of this guide for information about ensuring confidentiality of the investigation.

³¹ Section 66 defines the source agency for particular kinds of intelligence information.

8.2 PROTECTION FOR THE DISCLOSER

The PID Act provides for:

- » protection of the discloser's identity (see 8.2.1 below)
- » immunity from civil, criminal or administrative liability (see 8.2.2 below)
- » support and protection from reprisal (ss 13, 19 and 59 - see 8.5 and 8.6 below)
- » recourse to court for remedies for reprisal action (ss 14 – 16, see 8.7 below)

These protections and immunities apply not only to internal disclosures, but to external and emergency disclosures made in accordance with the PID Act.

Even if the discloser's report of wrongdoing turns out to be incorrect or is unable to be substantiated, they are still protected under the PID Act, provided their report meets the criteria for a public interest disclosure in s 26 (see 5.1.1), **and** they reasonably believe or believed at the time of the disclosure that the information tends to show disclosable conduct.

However, there are some limitations to the discloser's immunity from liability for making a public interest disclosure. An official will still be liable for knowingly making a disclosure of information that is false or misleading (s 11); or knowingly breaching a designated publication restriction without reasonable excuse (s 11A).³²

It should also be noted that making a public interest disclosure does not exclude a person from being reasonably managed or disciplined for any unsatisfactory performance or disclosable conduct on their part (s 12). This is discussed further in 8.2.2 below.

In addition to the protections under the PID Act, an agency should ensure that support is provided to the discloser where appropriate. The agency should also be mindful of their responsibilities towards anyone against whom an allegation has been made, and others who might be suspected to have made a disclosure. This is discussed further in 8.5 below.

Agencies are also bound by obligations under the *Privacy Act 1988* in relation to storing personal information securely and limiting its use and disclosure.

8.2.1 Protecting the discloser's identity

Agencies need to make every reasonable effort to protect the discloser's identity. In addition to the general secrecy provisions in the PID Act (s 65), there is additional and specific protection of the discloser's identity (s 20).

The discloser is entitled to make their disclosure anonymously (s 28(2) - see 4.1.5 of this guide and 8.2.1.3 below). If the discloser's identity is known to the authorised officer, the discloser may choose not to be identified as the source of the disclosed information when the principal officer is notified of it (s 44(1)(d) – see 5.2.5 of this guide).

Section 20 of the PID Act protects any information that could enable others to identify the person as the official who made the disclosure. The general intention of s 20 of the PID Act is to ensure that as far as possible, unless the discloser wishes to be identified as the source of the disclosed information, that fact should only become known to people who have a specific role in dealing with the disclosure. Those people should not directly or indirectly identify the discloser to anyone who does not have a similar need to know.

³²A 'designated publication restriction' means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the Family Law Act 1975 and the Migration Act 1958), witness protection and law enforcement mechanisms (see the full definition in s 8).

A public official who has obtained information that is likely to enable the identification of another person as someone who has made a disclosure may only use or disclose that identifying information:

- » with the discloser's consent (s 20(3)(e)); or
- » for the purposes of the PID Act (s 20(3)(a)); or
- » in connection with the Ombudsman or IGIS investigating a disclosure, or a complaint about the handling of a disclosure (s 20(3)(b) and (c)); or
- » if that particular identifying information has already been lawfully published³³ and the prior publication was lawful (s 20(3)(f)).

It is a criminal offence for a public official to use or disclose any information likely to enable the identification of a person as a discloser in any other circumstance (s 20(1)) A penalty of imprisonment for 6 months or 30 penalty units, or both, applies.

Some examples of circumstances where it may be appropriate or necessary to use or disclose information that is likely to identify the discloser include:

- » to investigate the disclosure effectively (for example, if the wrongdoing that was reported was directed solely against the discloser)
- » to protect the discloser against reprisals (for example, if there are concerns that it is impossible for them to remain in their current workplace).

In both of these situations, the use or disclosure of identifying information would be for the purposes of the PID Act and covered by the exception in s 20(3)(a).

8.2.1.1 Measures to protect the discloser's identity

When receiving a disclosure, authorised officers should emphasise to the discloser that the PID Act does not, and cannot absolutely protect their identity in all situations. As noted above, there are exceptions in s 20 of the PID Act that would allow identifying information to be used or disclosed. Furthermore, other staff may guess who made the disclosure once an investigation is under way, particularly if the discloser has previously complained about the issue to colleagues or flagged their intention to disclose.

It may be appropriate to seek the discloser's consent to reveal their identity to appropriate people. A discloser may consent to their identifying information being released to certain other people (such as the Ombudsman, another agency that has been allocated the disclosure or their workplace). If so, it is good practice to ask them to confirm this in writing. If they do not consent, it may not be practicable to protect their identity, particularly if it is widely known that the person has made the disclosure, or if identifying information needs to be disclosed for the matter to be effectively investigated.

Balancing the need to protect the discloser's identity with protecting them against reprisal and facilitating an investigation can be challenging. In order to protect a discloser's identity, agencies should:

- » limit the number of people who are aware of the discloser's identity or information that would tend to identify them
- » remind each person who has the information that they should keep it confidential and that unauthorised disclosure may be a criminal offence
- » assess whether anyone who is aware of the discloser's identity may have a motive to take reprisals against them or impede the progress of the investigation, and monitor the situation
- » ensure that the discloser can communicate with a support person, the authorised officer or investigator without alerting other staff.

³³ The term "published" is not defined in the PID Act. However, given the specific protections for the discloser's identity in the PID Act, a public official should be cautious before relying upon this particular defence.

If it is necessary or likely that the discloser's identity will become known during an investigation, the agency should explain this to them before the investigation starts. The agency should also take steps to protect the discloser against reprisal (see 8.5 below). An assessment of the risk of reprisal against the discloser should be conducted as soon as possible after the disclosure is received (see 8.5.3 below). The risk of reprisal against others who may be suspected to have made the disclosure should also be assessed.

8.2.1.2 *Can the discloser's identity be revealed to a court or tribunal?*

The requirement to protect a discloser's identity remains even where court or tribunal proceedings are involved. A former or current public official is not to be required to disclose to a court or tribunal identifying information that the person has obtained, or produce to a court or tribunal a document containing identifying information, except where necessary to give effect to the PID Act (s 21). This provision may be invoked where a person on trial is seeking information from an official about the identity of the discloser.

However, s 21 does not wholly prohibit disclosure of identifying information to a court or tribunal. If one of the exceptions in s 20(3) of the PID Act apply, an official may provide information to a court or tribunal that would identify the discloser. For example, where identifying information is relevant to a claim for compensation by the discloser, and the discloser consents, s 20(3)(e) permits an official to disclose that information to a court.

8.2.2 **Discloser's immunity from liability for making a disclosure**

A person who makes a public interest disclosure is not subject to any civil, criminal or administrative liability (including disciplinary action) for disclosing information in accordance with the provisions of the PID Act (s 10(1)(a)). However, if the official also tells that same information to other people, or has previously disclosed that information elsewhere, they are not protected from the consequences of making those other disclosures (unless those other disclosures were also public interest disclosures under the PID Act, i.e., an internal disclosure, an emergency disclosure, an external disclosure or a legal practitioner disclosure, as described in 2.7 of this guide).

This immunity from liability means, for example, that a person would not be committing an offence against the secrecy provisions of the *Crimes Act 1914* for making a disclosure in accordance with the PID Act. The person also has absolute privilege in proceedings for defamation in respect of the information they disclosed when making a public interest disclosure (s 10(2)(a)).

No contractual or other remedy may be enforced, and no contractual or other right may be exercised, against a person on the basis of them having made a public interest disclosure (s 10(1)(b)).

A contract to which the discloser is a party cannot be terminated on the grounds of them having disclosed information if that disclosure of information was made in accordance with PID Act (s 10(2)(b)).

These immunities do not apply if the discloser:

- » knowingly makes a statement that is false or misleading (s 11(1))
- » knowingly provides false or misleading information, or dishonestly produces forged or altered documents (s 11(2))
- » makes a disclosure knowing that it contravenes a designated publication restriction³⁴ and without a reasonable excuse for doing so (s 11A).

³⁴ A 'designated publication restriction' means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the Family Law Act 1975 and the Migration Act 1958), witness protection and law enforcement mechanisms (see the full definition in s 8).

The immunities under s 10 apply despite any provision in another Commonwealth law, unless that other provision is enacted after 15 January 2014 and is expressed to have effect despite s 10 or Part 2 of the PID Act (s 24).

It is important to note that making a disclosure about matters that include a discloser's own wrongdoing does not protect the discloser from liability for their wrongdoing (see 8.2.2.2 below).

8.2.2.1 Can immunity from disciplinary action be granted?

Making a public interest disclosure does not protect the person from liability for their own wrongdoing (s 12). However, the discloser or another witness may seek immunity from disciplinary action for providing information about improper conduct in which they are implicated. This is not a right or option under the PID Act, but may be something to be taken into account in any disciplinary proceedings or code of conduct investigation. It is up to the person with the power to take disciplinary action in each agency to decide how to exercise the discretion in such circumstances. The nature and seriousness of the witness's misconduct will be relevant to that decision.

8.2.2.2 What happens if proceedings are commenced?

If civil or criminal proceedings are instituted against someone because they made a disclosure, the discloser can claim immunity under s 10 of the PID Act (s 23). The discloser must be able to point to evidence that suggests a reasonable possibility that their claim is correct (s 23(1)(a)). It is then a matter for the person bringing the proceedings against the discloser to prove that the claim is incorrect (s 23(1)(b)). Other evidentiary and procedural matters that apply in such circumstances are also covered in s 23 of the PID Act.

8.3 PROTECTION FOR WITNESSES IN A PID INVESTIGATION

All current and former public officials are obliged to co-operate with a PID investigation (s 61).

The PID Act also provides protection for any person (including the discloser) who provides information when requested by a person conducting a PID investigation (see chapter 7 of this guide for information about PID investigations). These protections include immunity from criminal or civil liability (see 8.3.1) and protection from detriment and reprisal (see 8.5).

8.5 of this guide explains the principal officer's obligation to take reasonable steps to protect officials who belong to the agency from detriment, and threats of detriment relating to public interest disclosures. This protection obligation extends to witnesses, and other officials who may be suspected to have made disclosures.

8.3.1 Witness's immunity from liability for providing information

Any person who provides information to a person conducting a PID investigation will have immunity from any civil or criminal action for providing that information, provided it has been requested by the investigator and is relevant to the investigation (s 57(1)). This immunity means that the person may provide that information to the PID investigator without breaching any secrecy or confidentiality provisions in other laws, nor can providing that information to the investigator be a criminal offence.

However, the witness's immunity does not apply if the witness:

- » knowingly provides false or misleading information to the PID investigator, or dishonestly produces forged or altered documents (s 57(2)).
- » contravenes a designated publication restriction³⁵ (s 57(3)).

If the PID investigator is interviewing a witness, they must advise that person of their protections under s 57 of the PID Act (see 7.3.3.5 of this guide for more information about conducting interviews).

A witness who provides the PID investigator with information about their own conduct will not obtain immunity in respect of that conduct. Their immunity relates only to the act of providing the information to the investigator.

8.3.1.1 *What if the witness wants to raise other matters?*

Section 57 does not provide immunity for a person who provides information to a PID investigator without being asked to do so. Nor does it protect a person who provides information to the PID investigator which is not relevant to the investigation.

If a witness wishes to disclose information to the PID investigator about conduct unrelated to the investigation, the investigator should encourage the person to disclose that information to an authorised officer instead. The authorised officer can assess whether the information tends to show on reasonable grounds one or more instances of disclosable conduct and if so, allocate it for handling under the PID Act (see chapter 5 of this guide).

8.4 OFFICIALS EXERCISING POWERS OR PERFORMING FUNCTIONS UNDER THE PID ACT

Section 78(1) provides that a principal officer or their delegate, an authorised officer or a supervisor or manager of a discloser is not liable to any criminal or civil proceedings or any disciplinary action for acting in good faith in the exercise of functions and powers under the PID Act.

This protection does not apply to a contravention of a designated publication restriction³⁶ (s 78(2)). Nor does it affect a person's rights under the *Administrative Decisions (Judicial Review) Act 1977*, to seek review by a court or tribunal of any decision, conduct or failure to make a decision.

8.5 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.

³⁵ A 'designated publication restriction' means certain restrictions listed in the PID Act (s 8). They generally concern protecting the identity of people by such means as court or tribunal orders that information not be published (such as under the Family Law Act 1975 and the Migration Act 1958), witness protection and law enforcement mechanisms (see the full definition in s 8).

³⁶ See above

8.5.1 What is detriment and reprisal?

8.5.1.1 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).

8.5.1.2 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)).

8.5.1.3 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.

8.5.1.4 Managing the discloser's performance

Agencies should make clear in their PID procedures that making a public interest disclosure does not prevent supervisors and managers from addressing the discloser's unsatisfactory performance in the workplace. Nor does making a disclosure protect a person from the consequences of their own improper conduct if they are implicated in the wrongdoing they have reported (see 8.2.2 of this guide).

However, the agency may consider that the discloser's admission is a mitigating factor when considering disciplinary or other action against them, for example, if the discloser has brought to light information about serious wrongdoing in which they had minor involvement. This is a matter for the agency's discretion.

Disciplinary or other action against a discloser may be perceived as being taken in retaliation for making the disclosure, rather than reasonable action to address unsatisfactory performance.

If such action is being contemplated, the agency must be able to demonstrate clearly that:

- » there are sufficient grounds for the action
- » the action is reasonable and proportionate, and
- » the action is not being taken because the person made a disclosure.

The agency's usual procedures in relation to performance management and/or disciplinary action should be followed. A manager may also wish to obtain legal advice prior to taking any action against the discloser, to ensure that they are not left open to an allegation of taking a reprisal. All actions, conversations, decisions and reasons should be documented thoroughly.

8.5.2 Reprisal protections in the PID Act

A person who makes, or is suspected of making a disclosure under the PID Act is protected from reprisal in the following ways:

- » it is a criminal offence for anyone to cause detriment to a person because it is suspected or believed that they have made or will make a public interest disclosure (see 8.8 below)
- » a person who believes they are suffering or have been threatened with reprisal has the right to apply to court for an injunction to stop or prevent it (see 8.7 below)
- » a person has the right to apply for compensation for loss, damage or injury suffered from a reprisal (see 8.7 below).

The agency may be open to a claim for damages if it cannot show it took reasonable steps to prevent a reprisal (see 8.7 below).

8.5.3 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)(a)). 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.

8.5.3.1 *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.

8.5.3.2 *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 this guide for a suggested risk assessment framework.

8.5.3.3 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
- » 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.

8.5.3.4 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.

8.5.4 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?

8.5.4.1 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 one agency developed, which lists the types of detriment that might occur in that agency's work environment.

8.5.4.2 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.

8.5.4.3 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.

8.5.4.4 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 CONFLICT³⁷

<p>Threats or past experience</p>	<ul style="list-style-type: none"> » 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?
<p>Confidentiality unlikely to be maintained</p>	<ul style="list-style-type: none"> » 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 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 work unit? » 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?
<p>Significant reported wrongdoing</p>	<ul style="list-style-type: none"> » Are there allegations about individuals in the disclosure? » Who are their close professional and social associates within the organisation? » Is there more than one wrongdoer involved in the matter?* » Is the reported wrongdoing serious?*³⁸ » 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?
<p>Vulnerable discloser</p>	<ul style="list-style-type: none"> » 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 your organisation?*

³⁷ Adapted from NSW Ombudsman, *Managing risk of reprisals and conflict*, Public Interest Disclosure Guideline C4, p. 3.

³⁸ Risks of poor treatment for reporting wrongdoing identified by research (Brown, AJ (ed.) 2008, *Whistleblowing in the Australian public sector: Enhancing the theory and practice of internal witness management in public sector organisations*, ANU E Press, Canberra, pp. 137-164).

TABLE 2 — RISK ASSESSMENT MATRIX

Example only

(Each agency/workplace has specific features that will create different risks of reprisal/detriment)

	Identified risk event	Likelihood High/Medium/Low	Consequence Minor/Moderate/Serious	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 in workplace			
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)			

8.6 PRACTICAL SUPPORT AND PROTECTION STRATEGIES

8.6.1 Support for the discloser

Section 7 of the PID Standard provides that internal agency procedures must outline any support that will be made available to public officials who make disclosures relating to the agency.

A discloser who feels supported and sees the agency's procedures as fair is more likely to accept the agency's decision about their disclosure, even if the outcome is not what they wished. The agency should provide active support for the discloser, including:

- » acknowledgement for having come forward with a report of wrongdoing
- » an offer of support and information about what options are available
- » an assurance that the agency will take all reasonable steps necessary to protect them.

Although an investigator may be able to provide general information about the investigation process, they are unlikely to be the most appropriate person to support a discloser. Their role is to investigate matters objectively and impartially, and they may sometimes reach a conclusion that the discloser was not expecting, based on the evidence they have.

Apart from a supervisor or manager (if appropriate) or an authorised officer, the following sources of support can be very helpful to a discloser who is finding the process stressful:

- » peer support officers
- » family and friends
- » Employee Assistance Programs which provide access to professional counselling services.

Agencies should bear in mind that the discloser may not be the only person requiring support. Witnesses and any official who is the subject of allegations may also find the PID process stressful. They should also be advised of the arrangements that the agency has in place to support them, if required.

Some agencies may have established networks that can be utilised for support, such as a peer support or harassment contact officer network. Larger agencies may have professional staff such as welfare officers. It is appropriate to seek an official's consent before providing their details to an appropriate support person.

Disclosers and witnesses should be advised that they can discuss their general situation and the process with support people, but they should not provide information that would identify those alleged to have committed wrongdoing or other information that they have a duty to keep confidential.

The discloser (or any other public official) may also disclose information to a lawyer for the purposes of seeking legal advice or professional assistance in relation to making a disclosure (other than intelligence information, including sensitive law enforcement information), and this disclosure is authorised under the PID Act (see 2.7.8 of this guide).

8.6.2 What are the ongoing support requirements?

It is important that the authorised officer or other appropriate person involved in handling the disclosure contacts the discloser periodically to advise them of progress on their disclosure, taking into account confidentiality requirements (see 7.5.1 of this guide for notification requirements), and to ensure that the discloser is not suffering any detriment.

In particular, if a matter is not allocated for investigation or if an investigation is unable to substantiate their allegations, the discloser should be given sufficient information to help them understand the reasons (see Chapter 5 for further details).

8.6.3 How can an agency protect an official from reprisal?

The agency head's responsibility is to take "reasonable steps" to protect public officials who belong to their agency from detriment relating to public interest disclosures. Assessing the risk of reprisal action, and putting in place strategies to mitigate those risks is a proactive way to fulfil that obligation. The discloser and any witnesses should also be encouraged to report if they believe they are being or may be subject to a reprisal. That report may be made to an authorised officer, their supervisor or manager, or a support person in the agency.

Every allegation of reprisal must be taken seriously, recorded and responded to. All those involved in handling the public interest disclosure and aware of the discloser's identity need to monitor the work environment for signs of detriment and if necessary, take corrective action early. This may include the authorised officer, investigator, supervisor, manager and anyone else to whom the discloser has agreed to reveal their identifying information or who has that information for the purposes of the PID Act. If harassment or victimisation is ignored, problems are likely to escalate.

Responses to alleged reprisals will depend on their seriousness and other circumstances. Actions which may be taken to resolve workplace conflict include holding discussions with staff, providing guidance and support and closer supervision of the workplace for inappropriate workplace behaviours. Managers should also be conscious of setting an example for staff in their approach to public interest disclosures and support for disclosers. Action under an agency's bullying and harassment policy may be appropriate. In many agencies, conduct amounting to a reprisal will be a breach of the applicable code of conduct and can be dealt with under the agency's disciplinary system. Detrimental action may also be a criminal offence (see 8.8 below).

If the situation is potentially serious enough to require significant action such as transfer, relocation, a leave of absence, physical protection or an injunction, options should be discussed with the (specialist) area best able to assist in such PID-related matters in the agency.

The agency head's responsibility to take reasonable steps to protect public officials who belong to their agency from detriment relating to public interest disclosures applies even if the public official has made a disclosure relating to another agency, or if a different agency (such as the Ombudsman or IGIS) is investigating the disclosure.

8.7 ACCESS TO COURT

The PID ACT provides access to the Federal Court and Federal Circuit Courts for orders to address or prevent reprisal action (see 8.7.1 below).

The Fair Work Commission can also make some orders relating to a person's right to make a disclosure under the PID Act (see 8.7.2 below).

8.7.1 Federal Court and Federal Circuit Court

A person who has made a public interest disclosure can apply to the Federal Court or Federal Circuit Court for a range of orders where reprisal against them has been threatened or taken. Multiple orders may be made in relation to the same conduct (s 17). A person has the right to take such action even if a prosecution for a reprisal offence has not been or cannot be brought (s 19A).

8.7.1.1 Injunctions, apologies and other orders

Where the court is satisfied that another person took, threatened, or is taking or threatening, a reprisal, the court may grant an injunction:

- » restraining that person from taking or threatening to take a reprisal
- » requiring the person to do something, including making an apology, or
- » any other order the court considers appropriate (s 15).

The court may also make orders, including an injunction, against other people who are involved in taking, or conspiring to take, reprisal action (for example, by aiding or abetting the reprisal, inducing the conduct against the person or in any way being knowingly concerned in the conduct) (s 15(2)).

8.7.1.2 Compensation

A person has the right to apply for compensation for loss, damage or injury suffered from a reprisal or threat of reprisal (s 14). A claim can be made not only against the person causing the reprisal but also their employer if the reprisal is in connection with their position as an employee (s 14(1)) (the court may order that the employer is jointly or wholly liable).

The employer has a defence if they took reasonable precautions and exercised due diligence to avoid the reprisal or threat (s 14(2)).

8.7.1.3 Reinstatement

The court may order a person to be reinstated to their position, or a position at a comparable level, if satisfied that the person's employment was terminated (or purported to be terminated) wholly or partly as a reprisal for making or proposing to make a public interest disclosure (s 16).

8.7.2 Fair Work Commission


Section 22 of the PID ACT provides that making a public interest disclosure is treated as a workplace right under the *Fair Work Act 2009* (Cth) (the Fair Work Act). The Fair Work Act protects employees from any unlawful adverse action based on their workplace rights. The Fair Work Commission may make orders to remedy a breach of an employee's workplace rights.

As a result, if an employee suffers adverse treatment from their employer because they have made a public interest disclosure, they may apply to the Fair Work Commission for a remedy. To avoid duplication, a person cannot apply for an order under the PID Act if they have applied for an order in relation to the same conduct under ss 394 or 539 of the Fair Work Act (s 22A(1)). Similarly, a person who has made an application under the PID Act cannot apply to the court under the Fair Work Act (s 22A(2)). (This restriction does not apply if the other application has been discontinued or failed for want of jurisdiction s 22A(3)).

8.8 REPRISAL IS A CRIME

Taking reprisal action (described in 8.5.1 of this guide) is a criminal offence, punishable by imprisonment for two years or 120 penalty units, or both (s 19 of the PID Act). It is not necessary to prove that a person actually made or intended to make a public interest disclosure (s 19(2)): what is relevant is the intention and action (or omission) of the person who took the reprisal.

A person also commits an offence if they threaten to take a reprisal and either intend the threat to cause fear or are reckless about this occurring (s 19(3)). The threat may be express or implied, conditional or unconditional (s 19(4)). It is not necessary to prove that the person who was threatened actually feared that the threat would be carried out (s 19(3)).



If an agency has evidence that an official employed by the agency has taken or threatened reprisal action, it may refer that information to the Australian Federal Police (AFP). The AFP's website contains information about the procedure for government agencies to make reports, and contact details for initial enquiries or pre-referral advice.³⁹ The AFP will assess the reported information and decide whether and how to investigate it in accordance with their usual operational priorities. The agency should also consider whether other administrative or disciplinary action is appropriate in response to the conduct, consistent with the integrity arrangements for the agency concerned and given the position of the official whose conduct is in question.

³⁹<http://www.afp.gov.au/what-we-do/referrals>

9 The role of key agencies

9.1 Ombudsman

9.2 Inspector General of Intelligence and Security

9.3 Prescribed investigative agencies

9.1 OMBUDSMAN

The Ombudsman and the IGIS have oversight of the public interest disclosure scheme. In addition to handling public interest disclosures made about its own agency or public officials, the Ombudsman has a range of powers and functions under the PID Act:

- » determining standards with which agencies must comply
- » receiving notifications of allocations by agencies
- » receiving notifications from agencies where the discretion has been exercised not to investigate or not investigate further
- » receiving, allocating and investigating disclosures about other agencies
- » making decisions about extensions of time for agency investigations
- » providing assistance, education and awareness programs
- » preparing annual reports on the operation of the PID Act.

In addition, the Ombudsman is able to receive and investigate complaints about the handling of public interest disclosures under the *Ombudsman Act 1976*. The Ombudsman may also use own motion powers under the *Ombudsman Act 1976* to investigate public interest disclosure matters.

9.1.1 Determining standards

The Ombudsman has the power to determine PID standards in relation to particular matters covered by the Act (s 74). The PID Standard 2013 is a legislative instrument available at www.legislation.gov.au (also accessible from the Ombudsman's website).

Agencies must comply with the PID Standard when:

- » preparing procedures for dealing with internal disclosures made under the Act
- » investigating disclosures under the Act
- » preparing reports of investigations
- » providing information to Ombudsman for the purposes of the Ombudsman's annual reporting role (see 9.2.6 of this guide).

9.1.2 Receiving and allocating disclosures

A public official may make a disclosure directly to the Ombudsman about wrongdoing relating to any agency if they believe on reasonable grounds that it would be appropriate for the Ombudsman to investigate the matter. The only exception is if the matter relates to an intelligence agency: in that case the person may make a disclosure directly to the IGIS.

Unless special circumstances exist, the Ombudsman may allocate a disclosure it receives from a public official to another appropriate agency for handling under the PID Act, including the agency the disclosable conduct relates to or the agency the public official belongs to. This is consistent with a key

principle under the PID scheme that an agency should handle disclosures internally and that disclosers should be protected from reprisals.

9.1.3 When will the Ombudsman investigate a disclosure?

The Ombudsman may decide to investigate an internal disclosure about another agency that is made to an authorised officer in the Ombudsman's office or allocated (with consent) to the Ombudsman by another agency.

The Ombudsman will consider whether special reasons exist to conduct an investigation, or allocate the matter to the agency where the disclosable conduct is alleged to have occurred, or to a prescribed investigative agency with appropriate jurisdiction. If the Ombudsman does decide to investigate a disclosure, the investigative powers under the *Ombudsman Act 1976* will generally be used rather than the powers under the PID Act (see 7.2.1 of this guide). When investigating a disclosure the Ombudsman may, where appropriate, use the general investigative powers under the *Ombudsman Act 1976*. The broad powers include requiring the production of documents or other written records, requiring questions to be answered, examining witnesses on oath or affirmation, visiting premises and inspecting documents.

9.1.4 Making decisions about extensions of time

Agencies have 90 days to complete their investigation of a public interest disclosure, including preparing the investigation report (see 7.3.3.1 of this guide). The Ombudsman (or the IGIS in the case of intelligence agencies) can grant extensions of time either on request from a discloser or agency, or, alternatively, on their own initiative. In most cases, an extension is requested by the agency conducting the investigation.

Agencies should lodge an application for an extension of time to investigate well before the end of the 90 days where it is likely or known that the investigation will not be completed within the time limit (or well before a prior extension is about to expire and the agency needs a further extension). The Ombudsman's website www.pid.ombudsman.gov.au includes a form that agencies may use to apply for an extension. Agencies are encouraged to let the discloser know before they apply for an extension, and take the opportunity to explain why it is required and the steps that need to be taken to complete the investigation (see 7.5.1 of this guide).

The Ombudsman will not automatically grant an application for an extension. Each request is separately considered to determine if the additional time requested is reasonably necessary to ensure that the disclosure is properly investigated. The Ombudsman will also take into account a range of other factors including the availability of witnesses; the complexity of the investigation; the action already taken to progress it; and whether there have been any unreasonable or unexplained delays on the part of the agency. The Ombudsman will also take into account any views expressed by the discloser about the requested extension.

If an extension is granted, the Ombudsman or the IGIS will inform the discloser and give reasons for the extension (s 52(5)). This does not apply if contacting the discloser is not reasonably practicable. In cases where the Ombudsman or the IGIS don't have the discloser's identifying or contact details the agency handling the disclosure will be asked to notify the discloser. The principal officer of the handling agency must also let the discloser know, as soon as reasonably practicable after the extension is granted, about the progress of the investigation (s 52(5)).

If an extension is not granted, the agency is still required to complete the investigation and prepare a report. However, if that is not completed before the relevant time limit (i.e. 90 days, or such longer period was previously granted by the Ombudsman or IGIS) the discloser may be entitled to make an external disclosure under the PID Act (see 2.7.7 of this guide).

9.1.3 When will the Ombudsman investigate a disclosure?

The Ombudsman may decide to investigate an internal disclosure about another agency that is made to an authorised officer in the Ombudsman's office or allocated (with consent) to the Ombudsman by another agency.

The Ombudsman will consider whether special reasons exist to conduct an investigation, or allocate the matter to the agency to which the disclosable conduct relates, or to a prescribed investigative agency with appropriate jurisdiction. If the Ombudsman does decide to investigate a disclosure, the investigative powers under the *Ombudsman Act 1976* will generally be used rather than the powers under the PID Act (see 7.2.1 of this guide). Under the Ombudsman Act, the Commonwealth Ombudsman cannot investigate a disclosure about action taken in relation to a person's employment. These matters should be raised with the relevant Australian Government agency in the first instance.

When investigating a disclosure the Ombudsman may, where appropriate, use the general investigative powers under the *Ombudsman Act 1976*. The broad powers include requiring the production of documents or other written records, requiring questions to be answered, examining witnesses on oath or affirmation, visiting premises and inspecting documents. When the Ombudsman's office completes its investigation it will advise the principal officer of each agency to which the disclosure relates, and the discloser.

9.1.4 Making decisions about extensions of time

Agencies have 90 days to complete their investigation of a public interest disclosure, including preparing the investigation report (see 7.3.3.1 of this guide). The Ombudsman (or the IGIS in the case of intelligence agencies) can grant extensions of time either on request from a discloser or agency, or, alternatively, on their own initiative. In most cases, an extension is requested by the agency conducting the investigation.

Agencies should lodge an application for an extension of time to investigate well before the end of the 90 days where it is likely or known that the investigation will not be completed within the time limit (or well before a prior extension is about to expire and the agency needs a further extension). The Ombudsman's website www.pid.ombudsman.gov.au includes a form that agencies may use to apply for an extension. Agencies are encouraged to let the discloser know before they apply for an extension, and take the opportunity to explain why it is required and the steps that need to be taken to complete the investigation (see 7.5.1 of this guide).

The Ombudsman will not automatically grant an application for an extension. Each request is separately considered to determine if the additional time requested is reasonably necessary to ensure that the disclosure is properly investigated. The Ombudsman will also take into account a range of other factors including the availability of witnesses; the complexity of the investigation; the action already taken to progress it; and whether there have been any unreasonable or unexplained delays on the part of the agency. The Ombudsman will also take into account any views expressed by the discloser about the requested extension.

If an extension is granted, the Ombudsman or the IGIS will inform the discloser and give reasons for the extension (s 52(5)). This does not apply if contacting the discloser is not reasonably practicable. In cases where the Ombudsman or the IGIS don't have the discloser's identifying or contact details the agency handling the disclosure will be asked to notify the discloser. The principal officer of the handling agency must also let the discloser know, as soon as reasonably practicable after the extension is granted, about the progress of the investigation (s 52(5)).

If an extension is not granted, the agency is still required to complete the investigation and prepare a report. However, if that is not completed before the relevant time limit (i.e. 90 days, or such longer period was previously granted by the Ombudsman or IGIS) the discloser may be entitled to make an external disclosure under the PID Act (see 2.7.7 of this guide).

9.1.5 Providing assistance, education and awareness programs

The Ombudsman's functions include assisting principal officers, authorised officers and public officials in relation to the PID Act, and conducting education and awareness programs (s 62).

The Ombudsman does not provide legal advice to agencies or disclosers. However, the Ombudsman has published a range of guidance materials that give general information about the operation of the PID Act (including this guide). See the Ombudsman's PID website www.pid.ombudsman.gov.au.

Agencies and disclosers (both potential and actual) are also able to contact the Ombudsman's office by email (pid@ombudsman.gov.au) or phone (02 6276 3777) with any queries regarding the operation of the PID Act.

Staff from the Ombudsman's PID Team are available to give presentations on the operation of the PID scheme to agencies and other stakeholders on request, as well as delivering training to authorised officers. The Ombudsman's office runs open PID information sessions in various locations around Australia throughout the year, and has established PID communities in several Australian capital cities where PID practitioners can find out more about the PID scheme and share information with others. Details of upcoming events are published on the Ombudsman's PID website www.pid.ombudsman.gov.au.

9.1.6 Preparing annual reports

The Ombudsman must prepare a report to parliament each year on the operation of the PID Act (s 76). This report must include the following information for the financial year from agencies (s 76(2))

- » the number of public interest disclosures received by authorised officers of the agency
- » the kinds of disclosable conduct to which those disclosures relate
- » the number of disclosure investigations the agency conducted
- » the actions that the agency has taken in response to recommendations in reports relating to those disclosure investigations
- » the number and nature of the complaints made to the Ombudsman about the conduct of agencies in relation to public interest disclosures
- » information about the Ombudsman's performance of its functions under s 62 and the IGIS's performance of its functions under s 63.

Each year, the Ombudsman surveys every agency covered by the PID scheme to collect the information needed to prepare this report. Input from the intelligence agencies is coordinated through IGIS.

9.1.7 Assisting the Ombudsman

An agency must provide information requested by the Ombudsman for the purposes of preparing the Ombudsman's annual report under the PID Act (s 76). Agencies need to have regard to the PID Standard when providing information. The information may have deleted from it any information that is likely to enable the identification of any person, and any information which would result in the document being exempt under the FOI Act or result in it having a national security or other protective security classification (s 76(4)).

More broadly public officials are required to use their best endeavours to assist the Ombudsman in the performance of the Ombudsman's function under the PID Act (s 61(2)). This includes assistance with the Ombudsman's role in receiving notifications of allocation of public interest disclosures, assessing requests for extension of time for investigations and receiving notification and reasons from agencies where discretion not to investigate or not investigate further have been exercised.

Similar requirements apply to intelligence agencies assisting the IGIS under the PID Act (s 61(3)).

9.2 INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The IGIS performs a similar role as the Ombudsman in respect to the six intelligence agencies: the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Office of National Assessments, Defence Imagery and Geospatial Organisation, Defence Intelligence Organisation and Australian Signals Directorate. These roles include

- » receiving notifications of allocations by intelligence agencies
- » receiving notifications from intelligence agencies where the discretion has been exercised not to investigate or not investigate further
- » receiving, allocating and investigating disclosures about intelligence agencies
- » making decisions about extensions of time for intelligence agency investigations
- » providing assistance, education and awareness programs
- » assisting the Ombudsman in relation to the performance of the Ombudsman's functions under the PID Act.

The IGIS can use investigative powers under the *Inspector-General of Intelligence and Security Act 1986* when investigating disclosures under the PID Act, and can conduct own motion investigations.

9.2.1 IGIS: receiving, allocating and investigating

A public official may make a disclosure directly to the IGIS about wrongdoing relating to an intelligence agency if they believe on reasonable grounds that it would be appropriate for the IGIS to investigate the matter.

The IGIS will become involved in an investigation in similar circumstances to those of the Ombudsman, but in respect to matters relating to intelligence agencies.

The IGIS will look for specific reasons to conduct an investigation rather than allocating the disclosure to the relevant agency. In most instances it will be appropriate for the agency where the disclosable conduct is alleged to be occurring or have occurred to conduct the investigation.

More information about the role and functions of the IGIS are at www.igis.gov.au.

9.3 PRESCRIBED INVESTIGATIVE AGENCIES

Investigative agencies are those agencies listed in PID rules as well as the Ombudsman and IGIS (s 8). They are statutory agencies that have special powers to investigate matters within a particular jurisdiction. However, at the time of publication there are no prescribed investigative agencies.

Investigative agencies can use their investigative powers under their own legislation when dealing with a disclosure under the PID Act (s 49).

A person may make a disclosure directly to an investigative agency. An agency may allocate a disclosure to an investigative agency that has appropriate jurisdiction to consider the matter if the investigative agency consents.

Appendix 1 – Further information

A Reference Guide to the Public Interest Disclosure Scheme is available on the Ombudsman’s website, which provides a helpful overview of the scheme and the key responsibilities, process and timeframes under the PID Act. The Reference Guide is published under ‘Guides’ at <http://www.ombudsman.gov.au/about/making-a-disclosure/pid-resources>.

The following are useful sources of information to assist agencies and public officials in carrying out their responsibilities under the PID Act.

- » The Administrative Review Council has produced a range of Best Practice Guides on aspects of administrative decision-making, including natural justice requirements, assessing evidence and decision writing, available at www.arc.ag.gov.au.
- » The Australian Government Investigation Standards (AGIS) are available at www.ag.gov.au. All non-corporate Commonwealth entities must comply with the AGIS which sets out minimum standards for agency investigations involving suspected breaches of the law. It has useful information on such topics as investigation planning, interviewing witnesses and finalising investigations.
- » The PID Act and PID Standard on the Federal Register of Legislation available at www.legislation.gov.au.
- » For information about the role and functions of the IGIS, see www.igis.gov.au.
- » For information about breaches of the APS Code of Conduct, see www.apsc.gov.au.
- » Information about Australian workplace rights and rules and the role of the Fair Work Ombudsman is at www.fairwork.gov.au.
- » More information on the PID scheme, including fact sheets and guides, is on the Ombudsman’s website at www.pid.ombudsman.gov.au.

For further information about see
www.pid.ombudsman.gov.au.



PID information

LINE 02 6276 3777
FAX 02 6276 0123
EMAIL PID@ombudsman.gov.au
WEB www.pid.ombudsman.gov.au
POST GPO Box 442, Canberra ACT 2601



COMMONWEALTH
OMBUDSMAN

Guidance for

C **OMPLAINT HANDLERS**

on dealing with risks of harm



Guidance for complaint handlers on dealing with risks of harm

PURPOSE

This document aims to give complaint handlers confidence in handling complainant behaviour that poses a risk of harm to themselves or others.

By sharing these practical guidelines, we hope that education providers and other agencies can improve their responsiveness and accessibility to all complainants. This guide has 4 sections:

- responding to someone at risk of self-harm or suicide
- responding to someone who indicates they pose a risk of harm to someone else
- tips for supporting employees who've dealt with the risks, and
- some printable quick reference guides.

BACKGROUND

In any job involving people, you may find yourself dealing with someone who is considering self-harm, suicide or harming someone else. Dealing with this situation can be confronting and difficult, so it is important to have guidance available.

Any indication that a person intends to harm themselves or others must be taken seriously, assessed quickly and responded to appropriately. Generally, staff responding will not be mental health professionals, so it is not appropriate to try and guess whether the risk is genuine. All risks should be taken seriously. Responding can include contacting police or emergency services depending on the level of risk. Other options include encouraging the person to engage with a doctor, mental health professional or support services, or other appropriate support people.

There are many reasons why a person might experience the thought or impulse to self-harm or suicide or display behaviours of concern. Our focus in this guide is addressing the specific behaviour, meaning someone's observable conduct and what they are communicating, not the person's motives for their behaviour. This guide focuses on ensuring you have the tools to respond to the behaviour in a sensitive way.

PRIVACY AND CONFIDENTIALITY

Education providers and other agencies should always prioritise a person's right to privacy and confidentiality. However, when a person expresses thoughts or impulses to self-harm or harm others, and you reasonably believe there is a safety risk, you may have a duty of care to share information without that person's consent.¹

¹ Under the *Privacy Act 1988*, personal information can be disclosed in situations where it is necessary to prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Definitions

Risk – the likelihood that someone may cause physical harm to themselves through intentional activity (e.g. cutting or suicide).

Threat – an indication given by someone that they may cause physical harm to a specific person or group of people.

Employee – for the purposes of this document, assume this also includes any worker to whom you have work health and safety obligations but may not be defined as an employee. For example anyone who carries out work for a Person Conducting a Business or Undertaking (PCBU) such as an employee, a contractor, employee of a labour hire company, an apprentice or trainee, a student gaining work experience, an outworker or a volunteer.

General disclaimer

To the extent permitted by law, the Commonwealth Ombudsman's Office will in no way be liable to you or anyone else for any harm, loss or damage, however caused (and whether direct, indirect, consequential or economic) which may be directly or indirectly suffered in connection with the use of these Guidelines.

While we make every effort to make sure the information in these Guidelines is accurate and informative, the information does not take the place of professional or medical advice.

You must make your own assessment of the information contained in these Guidelines and, if you choose to rely on it, it is wholly at your own risk.

Self-harm, including suicide

We do not refer to expressions of intention to self-harm or commit suicide as threats, as this may create the perception that expressing these intentions is intended to manipulate or unfairly influence.

Instead, we refer to the possibility that a person will self-harm or commit suicide as a risk. This reflects the distress, helplessness and personal risk of those experiencing thoughts of suicide and self-harm.

RESPONDING TO RISKS OF SELF-HARM OR SUICIDE

The following procedure is intended as a guide. You may not need to follow the steps in order. You may skip steps depending on the circumstances.²

When communicating with a distressed person it can help to:

- provide an opportunity for the person to express themselves
- acknowledge their feelings of anger, frustration, sadness or disappointment
- encourage the individual to think about wellbeing strategies or support they can access.

Workplace supervisors are responsible for supporting employees to assess and manage risks. Employees should raise any concerns about a person's safety with a supervisor.

1 Do something now 2 Gain rapport

When communicating with people in crisis or distress:

- respond calmly and be aware of your tone of voice
- acknowledge their emotions
- show them you're listening by paraphrasing, summarising and asking them questions about what they're telling you
- give information in small amounts
- be supportive without claiming to know how they feel.

3 Be there for the person

Listen to words or phrases that may indicate a level of suicide risk. Some examples are:



'I want to kill myself...'

'I just don't think there's any point anymore...'

'It won't matter after tomorrow...'

'Things would be easier if I wasn't around...'

² This procedure draws on Lifeline's toolkit: *Helping someone at risk of suicide*: Toolkit downloads - Lifeline Australia: <https://www.lifeline.org.au/resources/toolkit-downloads/>

4 Validate and support 5 Normalise feelings

Suicidal thoughts are common among people who experienced significant trauma. An important reflection to people who are suicidal is to normalise their feelings:



'Suicidal thoughts are not unusual for someone who's been through what you have experienced.'

'Thank you for letting me know you're feeling this way. It's a very normal way to be feeling in these circumstances. It must have taken you a lot of strength to tell me.'

'Thank you for sharing this with me. I know it must be difficult to talk about these feelings. I am very concerned about your safety and I want to help you.'

6 Ask direct questions

If you don't ask a person directly if they are suicidal, you can't know their level of risk. You should ask a person to expand on what they mean when they say something which may indicate they are thinking of committing suicide or harming others – even if it sounds ambiguous.

If you feel there is a level of suicide risk, an example of a response could be:



'You are telling me that you just don't think there's any point anymore... I am very concerned about you. Are you thinking of killing yourself?'

7 Get info 8 Establish immediacy 9 Assess risk

In the next steps, you need to gather information and decide what the level of risk is. Some questions are provided to help you gather this information in the **Assessment Conversation Template: Risk of Self-harm and Suicide** attached.

As with everything in this guide, this process doesn't always have to be followed in order.

It is important to find out whether the person intends to act on their thoughts and to assess immediacy and risk.

The following questions may be helpful:



'You mentioned you are thinking of suicide. Are you thinking of acting on those thoughts?'

'Have you thought about how and when you plan to kill yourself?'

'Have you ever harmed yourself on purpose?'

'Do you have access to any weapons?'

'What are you planning to do?'

● Check safety 11 ● Check supports

Identifying the person's support resources can be useful at any stage during the interaction. Talking about support can help ground the person and move them away from suicidal thinking. Identification of support to contact is also useful information if the person is assessed as high risk.

Talk about what support they can access to stay safe and get help. How can you help the person draw on connections with family, friends, personal coping strategies?

It is also helpful to try and get contact details for the person's GP, counsellor, psychologist or psychiatrist in case it is appropriate to request assistance or intervention. If speaking on the phone suggested questions could be:



'Are you with anyone at the moment?'

'Is there someone you can call to seek support?'

● Duty of care 13 ● Consult and decide action

If the person states they are going to harm themselves or harm someone else and the risk may be imminent, you need to tell them:

- you will discuss the conversation with your supervisor
- you may need to contact other services such as police and mental health services, and
- you may need to contact the person's emergency contact, their GP, counsellor, psychologist or psychiatrist (if you have the details available).

For example:



'I am concerned for you and I need to make sure you have support. I may contact someone to check on your safety.'

If the person is on the phone and they hang up during the call, speak to a supervisor about how to proceed.

Where appropriate, you should consider getting help from colleagues and supervisors to manage people who pose a risk of harm to themselves or someone else. This could include signalling to another person to alert them to the nature of the call or interaction and that assistance is required.

● Take action 15 ● Refer

In consultation with a supervisor, you may need to notify another agency (for example: police, ambulance, child protection, mental health service, or the National Security Hotline).

You may also provide the contact details for 24-hour telephone support services:

- Lifeline 24 hr Counselling Service: **13 11 14**
- Beyond Blue: **1300 224 636**
- Suicide Call Back Service: **1300 659 467**

If you don't think the risk is imminent and you won't be notifying another agency, still provide the contact details above.

16 Defuse and debrief 17 Self-care

Working with people in crisis can be distressing. As everyone processes these interactions differently, there are a variety of different options available. Some examples are:

- undertaking your own personal self-care strategies
- informal/formal debriefing with supervisors or colleagues.

Make sure you are aware of the direct impacts of managing crisis situations and the potential for experiencing vicarious trauma. You should encourage any person impacted to seek appropriate help and support, and seek support yourself.

IN SUMMARY

If a person says something that indicates they may be thinking of harming themselves, ask them a direct question about what they intend to do. If you think there may be an imminent risk of self-harm or suicide, try to gather as much information as possible to inform appropriate referral or intervention.

If a person writes something in an email or a letter that indicates they may be thinking of harming themselves, you should attempt to contact the person by telephone, where possible. If this is not possible, discuss this with your supervisor. You may need to arrange emergency intervention depending on the information in the email or letter.

If you are in a face-to-face situation with someone who raises the risk of self-harm, follow the same procedures to assess the risk as on the phone, and escalate as required. Unless there is a risk to your own safety, try not to leave the person on their own.

Remember it is important to provide training to any staff or person who may be required to respond to risks of harm and keep records of any incidents.

Threats of harm to staff and others

In this section of the guidelines, we refer to expressions of an intention to cause harm to others as **threats**. This is appropriate as the intention is to control an outcome by making others feel threatened.

PROCEDURE FOR RESPONDING TO THREATS OF HARM

The following procedure is intended as a guide for responding to threats to yourself, your colleagues or a third party. This can include hostility, aggression and assaults. You do not need to follow the steps in order. You may skip steps depending on the circumstances.

Where employees are at risk due to dangerous or aggressive behaviour during or as a direct result of their work, the organisation must take immediate action to protect their health and safety. This is in accordance with duty of care and workplace health and safety obligations.³

Employees should report any threat of harm to a supervisor, whether it is made face-to-face, on the phone or in writing. The supervisor should decide what the response is, and this may include contacting the police and requesting their attendance.

If an employee is confronted with someone displaying threatening behaviour, they should try to de-escalate the behaviour. If at any time the employee feels their safety is at risk, they should remove themselves from the situation immediately and seek assistance. Remember not to speculate on the motives for someone's behaviour. Address the behaviour, not the person.

If duress alarms are available, staff should follow procedures to use them. Consider developing simple phrases or codes which alert others in the team of an emerging situation where assistance may be needed.

1 Do something now 2 Recognising danger signals and assessing risk

The following signals may indicate that a person could become aggressive or violent:

- **Appearance:** seems intoxicated or is carrying something that could be used as a weapon.
- **Physical activity:** restless or agitated, pacing, hostile facial expressions, has entered non-public area of the office.
- **Speech:** loud, swearing or abusive, slurred.

The signals above may alert you to potential danger, but other explanations need to be considered. For example, slurred speech may be caused by a speech impairment and agitation and pacing by anxiety. Do not automatically conclude that a person intends harm by displaying these behaviours.

³ [Model-Guidelines-For-Managing-and-Responding-to-Threats-Aggressive-Behaviour-and-Violence.pdf \(nsw.gov.au\)](#) P 26, *Work Health and Safety Act 2011*(Cth), and corresponding legislation in each State/Territory.

The strategies below will help you manage any risk associated with responding to a person displaying those signals, while still treating them with respect and concern for their problem:

- If you are in a public space speaking to a distressed person, ensure you are not alone. If available, ensure you are being monitored on security screens.
- If meeting with a person who is displaying aggressive or intimidating behaviour, do not keep them waiting before attending to them.
- Ask a colleague to attend the meeting with you.
- If possible, use a room where you can attend to the person in a calming, low stimulus environment and position yourself near an exit or safety alarm.
- Use calm words, tone and body language. Learn and use de-escalation and distraction strategies outlined below.
- Ensure someone else is aware of the situation. If possible, restrict access to the area by other persons until the situation calms down.
- If you feel you are in danger, remove yourself as quickly as possible. Walk through the nearest door to a secure area and let others know of the risk.
- If safe to do so, encourage the person away from the premises or disconnect the person from the phone call. If possible, leave a route for the person to follow where they will not feel like they are trapped or cornered, as this may increase their agitation.

3 Defuse the situation 4 Using de-escalation strategies

The aim of using de-escalation techniques is to calm the person and manage the physical environment. You should aim to:

- stay calm and adopt a neutral, open posture
- speak slowly and clearly, even if the person is shouting
- acknowledge the grievance and communicate a willingness to see what can be done.

For example:



'I can hear you are very angry about ...; or 'I am concerned about you and would like to help you'

- clarify any statements that suggest a risk of harm to the person or someone else by repeating what the person has said. For example:



'You have just said you will'

- ask open ended questions to keep the dialogue going. A question about the facts can change a person's focus:



'Can you tell me about ...'

If possible, it can also be useful to identify someone the person normally relies on for support.

5 Respond to ensure safety of all parties

6 Raising your concerns with the person and with others

If the person continues to exhibit unacceptable behaviour take the following actions:

- if you feel you are in danger, activate a safety alarm (if available), or leave the room and request assistance
- inform the person what the consequences of their unacceptable behaviour will be. For example:



'If you continue to speak/act like that, I will stop this conversation.'

- inform the person of the actions you will take in response to their continued behaviour/words:



'You have just said that you will...' (repeat the person's language). 'Our policy here is that all threats must be taken seriously and responded to. I will now inform a supervisor that you have said you will...' (use the words the person has used). 'If you continue to make those comments, I will request that you leave the premises.'

7 Discuss with your supervisor

8 Reviewing your responses to the situation

With your supervisor, identify strategies for future interactions with the person, for example a follow up call and referrals to other services.

You may also provide 24-hour telephone support services:

- Lifeline 24 hr Counselling Service: **13 11 14**
- Beyond Blue: **1300 224 636**

9 Defuse and debrief

10 Self-care

It is important to provide training to employees who may be exposed to threats of harm and to keep records of any incidents.⁴

⁴ Examples of procedures and all following templates are from Office of the Commonwealth Ombudsman Policy and Procedures for Responding to Risks of Harm and Threats to Others.

Employee Support

After all action to manage the risk is completed, supervisors should offer and provide support. Defusing and debriefing are 2 support strategies for staff who deal with difficult situations.

DEFUSING

- initial response post-crisis (within 12 hours)
- check the wellbeing of the person/employee involved, offering initial support
- arrange debriefing and follow-up sessions.

Defusing is designed to assist people to manage any distress in the short-term and address immediate basic needs. It is very important to do this as soon as possible, on the day of the incident, before leaving work. Defusing is done informally and usually by peers (small group support). The aim is to stabilise the responses of employees involved in the incident and provide an opportunity to express any immediate concerns.

Guided discussion and the opportunity to ask questions can help ground everyone involved in managing the incident. For example:



'What is one 'self-care' activity you can do for yourself after you finish work today?'

Defusing activities include:

- briefly reviewing the event
- discussing questions and concerns
- identifying current needs
- offering advice, information and handouts on referrals and support agencies.

DEBRIEFING

Debriefing helps people deal with reactions to a distressing incident, reflect on its impact, and discuss whether additional support or action is required. It can help people begin processing the event and bring closure.

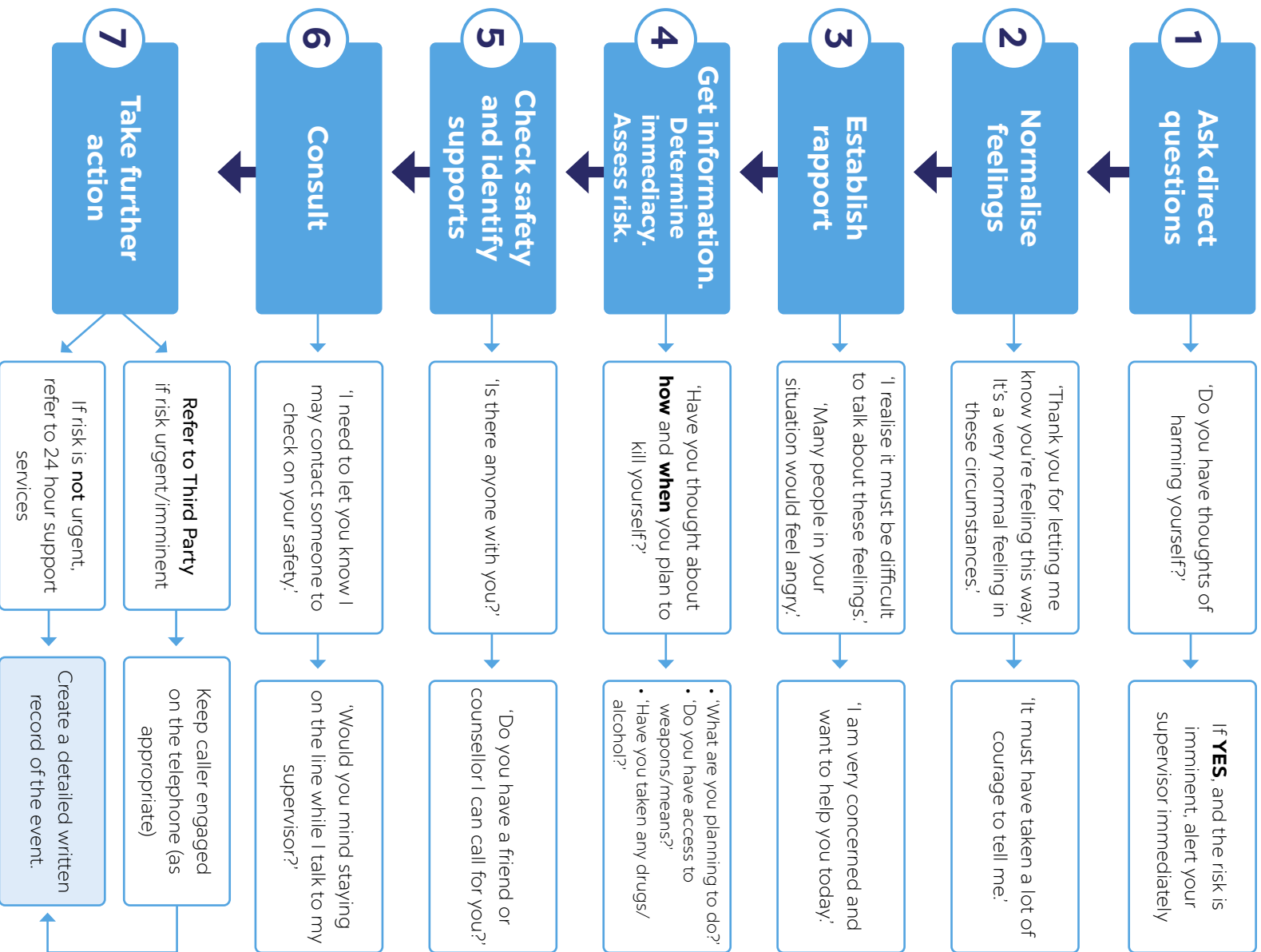
Employees should have the opportunity to debrief as soon as possible, but no longer than 72 hours after the initial incident.

Encourage your employees to debrief with a senior staff member or colleague, or to use facilitated debriefing support such as counselling services. It can be done informally or formally, depending on the needs of those involved.

The following steps may act as a facilitation guide, but remember to tailor the discussion to employee needs and the circumstances surrounding the incident:

- acknowledge the role played by all involved
- invite the person to discuss both the positive and negative elements of the experience
- ask open-ended questions that help the person explore the facts, thoughts and sensory experience related to the event
- allow expression of thoughts, emotions and experiences associated with the event without judgement
- identify the incident's impact on the person to determine whether follow-up support is required
- advise what additional support is available such as counselling services facilitated by the organisation.

ATTACHMENT A – Quick Risk Assessment Tool RESPONDING TO RISKS OF SELF-HARM OR SUICIDE



ATTACHMENT B – Assessment Conversation Template

RISK OF SELF-HARM OR SUICIDE

The person has told you they have a current plan of self-harm. Repeat back what they tell you:



'You have told me thank you for sharing this with me. I know it must be difficult to talk about these feelings. I am very concerned about your safety and I want to help you.'

Supervisor Name: _____ Supervisor Number: _____

Step	Question	Response
1. Name	What is your full name? <i>(if not known)</i>	
2. Contact details	If we lose phone connection, what number should I use to phone you back?	
	Where are you now? <i>(If person is unsure of whereabouts, ask: "What can you see/nearest building/street?")</i>	
3. Get Information	What are you planning to do? <i>(If the person indicates they are planning suicide using weapons, identify what type of weapon and if they have access to it.)</i>	
	When?	
4. Assess Risk	Is there anyone with you? Name/relationship/their contact details.	
	Have you been taking any drugs/ alcohol? What/Quantity?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> I don't know
	Are you on any medication? Have you taken it today? How much have you taken? Name/Quantity/Method?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> I don't know
	Have you ever been diagnosed with any mental health issues?	
	Have you ever felt suicidal before?	
	When you felt like this in the past, how did you make yourself feel more positive?	
5. Immediate Response	Do you have a counsellor/ psychologist/GP/support person I can call for you?	

Continued next page

Risk of self-harm or suicide: assessment conversation template (cont.)

NOTES:

--

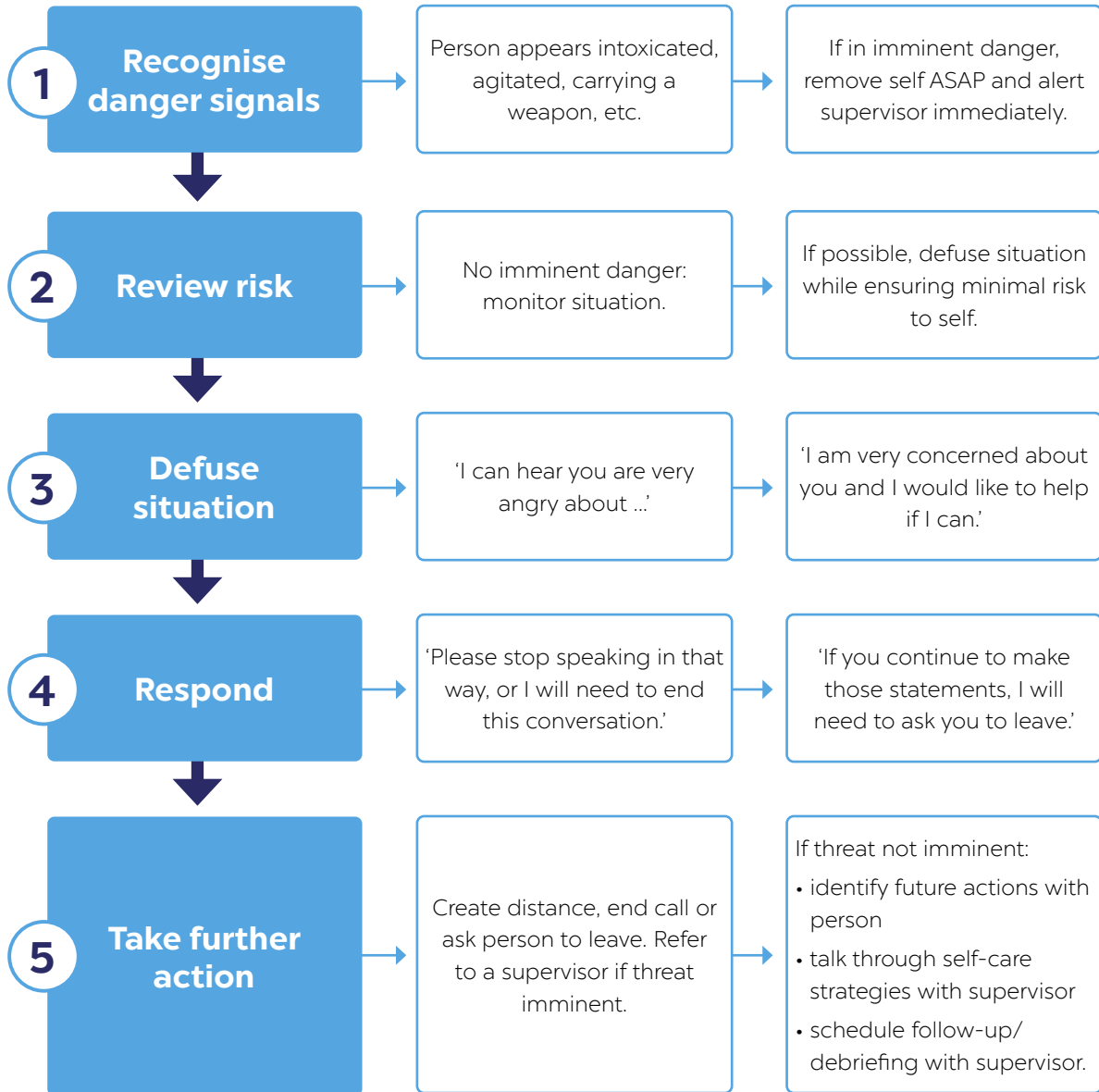
Referral services

- Emergency Services **000**
- Lifeline 24 hr Counselling Service **13 11 14**
- Beyond Blue **1300 224 636**

NOTE: Where there is a suicide in progress or the person indicates an imminent plan to harm themselves, try to maintain communication with the person and seek assistance to contact emergency services, requesting an ambulance and/or police.

ATTACHMENT C – Quick Assessment Tool:

RESPONDING TO THREAT OF HARM TO OTHERS (INCLUDING FACE-TO-FACE)



ATTACHMENT D – Assessment Conversation Template

THREAT OF HARM TO OTHERS

The person has told you they have a current plan to harm another person(s). Repeat back what they tell you:



'You have told me I am concerned about what you just said, and I need to remind you that we have a duty of care to report any threat of harm to others. Can you tell me more about what you are planning to do?'

Supervisor Name: _____ Supervisor Number: _____

Step	Question	Response
1. Name	What is your full name? <i>(if not known)</i>	
2. Contact details	If we lose phone connection, what number should I use to phone you back? Where exactly are you now?	
3. Validate feelings	<i>'Anger is a very normal emotion, and you have every right to be angry. Can we find a way to use this anger in a more useful way which will help you and keep you safe at the same time?'</i>	
4. Get information and assess risk	Try to use the wording below to establish the level of risk.	Try to capture the person's words as exactly as possible. This will be important if referred to police.
	What are you planning to do?	
	When are you planning to do this?	
	Who are you thinking about doing this to?	
	Where are you thinking about doing this?	
	Why are you thinking about doing this?	
5. Immediate response	Do you have any weapons? Is there anyone with you?	
	Is there something we can do to stop you from doing this?/change your mind about doing this? Is there anyone I can call who might be able to help you work through this anger without putting yourself at risk?	
NOTES:		

Crisis Intervention

Emergency Services

000

National Security Hotline

1800 123 400

Mental Health Crisis and Assessment Treatment Teams (CATT) vary for each State/Territory. There is more information and contact details available at:

healthdirect.gov.au/crisis-management

If you work with complainants in a particular State or Territory, you may wish to add the name and contact number for the appropriate CATT here:

24 Hour Helplines

Lifeline: **13 11 14**

Beyondblue: **1300 22 4636**

Suicide Call Back Service: **1300 659 467**

1800-Respect (sexual assault, family and domestic violence):

1800 737 732



COMMONWEALTH
OMBUDSMAN